Office for Nuclear Regulation

**New Reactors Division**

# Step 4 Assessment of Control and Instrumentation for the UK Advanced Boiling Water Reactor

Assessment Report: ONR-NR-AR-17-017
Revision 0
December 2017

Published 12/17

*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

Hitachi-GE Nuclear Energy Ltd (Hitachi-GE) is the designer and GDA Requesting Party for the United Kingdom Advanced Boiling Water Reactor (UK ABWR). Hitachi-GE commenced Generic Design Assessment (GDA) in 2013 and completed Step 4 in 2017.

This assessment report is my Step 4 assessment of the Hitachi-GE UK ABWR reactor design in the area of Control and Instrumentation (C&I).

The scope of this Step 4 assessment is to review the C&I aspects of safety and security of the UK ABWR by examining the evidence supporting the claims and arguments made in the submission, building on the assessments already carried out for Step 3, by Hitachi-GE. In addition, I have provided a judgement on the adequacy of the C&I information contained within the Pre-Construction Safety Report (PCSR) and supporting documentation.

My assessment conclusion is that:

- The PCSR and supporting documentation submitted by Hitachi-GE in GDA Step 4 adequately identify and justify the main C&I systems and equipment important to safety expected in a modern nuclear reactor.
- The principal design and implementation standards used by Hitachi-GE for all C&I systems and equipment important to safety are broadly in accordance with those expected in the nuclear sector in the UK.
- The C&I safety case for the sampled key C&I systems and platforms is broadly in line with ONR's expectations.
- The cyber security principles expected to be considered as part of the justification of the adequacy of the C&I systems important to safety for a modern nuclear power plant have been established.
- Hitachi-GE has adequately addressed the C&I Regulatory Observations raised by ONR in previous GDA steps.
- The safety case submitted by Hitachi-GE achieves the purpose of GDA, i.e. to de-risk future activities in the development of the UK ABWR C&I detailed design.

My judgement is based upon the following factors:

- assessment of the C&I architecture - primarily for those main systems important to reactor safety proposed for the UK ABWR;
- assessment of the key submissions, including the PCSR Chapter 14 and the Basis of Safety Cases for the overall UK ABWR C&I architecture and key systems;
- sampling of the key supporting documents, providing the evidence to support claims and arguments identified in the C&I safety case; and
- discussions with other relevant disciplines (including, but not limited to, Fault Studies, Probabilistic Safety Assessment, Human Factors and Internal Hazards) regarding the overall claims on the UK ABWR C&I systems important to safety.

In my assessment I have not identified significant technical concerns that require GDA Issues to be raised. However, I made a number of observations during my assessment of the GDA submissions. Because these matters do not undermine the generic safety submission but require licensee input/decision at a specific site, these are for a future licensee to consider and take forward in their site-specific safety submissions. These C&I assessment findings cover the following areas:

- the justification of the FPGA used for the Class 1 SSLC system as the detailed design develops (e.g. independent verification at the board level, verification of the FPGA configuration, verification of macros, tools, maintenance terminal);

- considerations in the C&I detailed design development of key activities and analyses, to confirm the principles justified in GDA (e.g. regarding diversity and standards compliance);
- development of adequate intelligent customer arrangements covering key areas of interest for ONR (e.g. smart device justifications and surveillance of third party activities);
- consistency between claims in Fault Studies and Probabilistic Safety Assessment and the engineering substantiation in C&I (e.g. regarding reliability or resilience of the plant control system to common mode failure);
- testing and maintenance, to account for the detailed design information;
- considerations of the development of the human machine interface (HMI) in areas of particular interest such as transfer switches and alarms; and
- consideration of a number of technical observations out of scope for GDA but considered important in licensing, to ensure the clarity and consistency of the safety case.

Overall, based on the samples undertaken, I am satisfied that the claims, arguments and evidence laid out within the PCSR and supporting documentation submitted as part of the GDA process present an adequate safety case for the generic UK ABWR design in the area of Control and Instrumentation. For this reason, I recommend the UK ABWR should be awarded a Design Acceptance Confirmation (DAC).

## LIST OF ABBREVIATIONS

| | |
|---|---|
| ACS | Reactor/Turbine Auxiliary Control System |
| ALARP | As Low As Reasonably Practicable |
| A-PPRM | Axial Peaking Power Range Monitor |
| BBCR | Backup Building Control Room |
| BSC | Basis of Safety Case |
| B/B | Backup Building |
| CAE | Claim, Argument and Evidence |
| CBSIS | Computer Based Systems Important to Safety |
| CCF | Common Cause Failure |
| CDF | Core Damage Frequency |
| CNS | Civil Nuclear Security |
| COTS | Commercial off the shelf |
| CSA | Conceptual Security Arrangements |
| C&I | Control & Instrumentation |
| DAC | Design Acceptance Confirmation |
| DBA | Design Basis Accidents |
| DBT | Design Basis Threat |
| EA | Environment Agency |
| ECCS | Emergency Core Cooling System |
| EE | Electrical Engineering |
| EH | External Hazard |
| EMI | Electro-Magnetic Interference |
| FC | Fuel and Core |
| ffpy | failure frequency per year |
| FPGA | Field Programmable Gate Array |
| FMEA | Failure Mode and Effect Analysis |
| FS | Fault studies |
| FSA | Functional Safety Analysis |
| GDA | Generic Design Assessment |
| HIACS | Hitachi Integrated Autonomous Control System |
| HF | Human Factors |
| Hitachi-GE | Hitachi GE Nuclear Energy Ltd |
| HLSF | High Level Safety Function |
| HMI | Human Machine Interface |
| HWBS | Hardwired Backup System |
| IAEA | The International Atomic Energy Agency |
| IBD | Interlock Block Diagram |
| IC | Intelligent Customer |

| | |
|---|---|
| ICBM | Independent Confidence Building Measure |
| IEC | International Electrotechnical Commission |
| IEMO | Initiating Events of Malicious Origin |
| IH | Internal Hazard |
| INPO | The Institute of Nuclear Power Operations |
| MCR | Main Control Room |
| MDEP | Multi-national Design Evaluation Programme |
| ME | Mechanical Engineering |
| NL | Nuclear Liabilities |
| NRW | Natural Resources Wales |
| NSEDP | Nuclear Safety and Environmental Design Principles |
| ONR | Office for Nuclear Regulation |
| PCntlS | Plant Control System |
| PCS | Plant Computer System |
| PCSR | Pre-construction Safety Report |
| PE | Production Excellence |
| pfd | probability of failure on demand |
| PSA | Probabilistic Safety Assessment |
| PSR | Preliminary Safety Report |
| RGP | Relevant Good Practice |
| RI | Regulatory Issues |
| RO | Regulatory Observation |
| RP | Requesting Party |
| RQ | Regulatory Query |
| RSS | Remote Shutdown System |
| RVI | Reactor Vessel Instrument System |
| SA | Severe Accident |
| SA C&I | Severe Accident Control & Instrumentation |
| SACS | Safety Auxiliary Control System |
| SAPs | Safety Assessment Principles |
| SCDM | Safety Case Development Manual |
| SDD | System Design Description |
| SFC | Safety Functional Claim |
| SI | Structural Integrity |
| SIS | System Important to Safety |
| SoDA | Statement of Design Acceptability |
| SPC | Safety Property Claim |
| SSC | System, Structure (and) Component |
| SSLC | Safety System Logic and Control |

| | |
|---|---|
| SW | Software |
| TAG | Technical Assessment Guide |
| TO1 | Technical Observation (higher importance) |
| TO2 | Technical Observation (lower importance) |
| TR | Topic Report |
| TSC | Technical Support Contractor |
| J-ABWR | Japanese Advanced Boiling Water Reactor |
| UK ABWR | United Kingdom Advanced Boiling Water Reactor |
| URC | Unacceptable Radiological Consequence |
| WENRA | Western European Nuclear Regulators' Association |

## TABLE OF CONTENTS



### Figures



### Tables



### Annexes

# 1 INTRODUCTION

## 1.1 Background

1. Information on the GDA process is provided in a series of documents published on the ONR website (Ref. 1). The expected outcome is a Design Acceptance Confirmation (DAC) for ONR and a Statement of Design Acceptability (SoDA) for the Environment Agency (EA) and Natural Resources Wales (NRW).

2. The GDA Step 3 summary report is published on the ONR website (Ref. 2).

3. Hitachi-GE Nuclear Energy Ltd (Hitachi-GE) commenced GDA in 2013 and completed Step 4 in 2017. The Step 4 assessment is an in-depth assessment of the safety, security and environmental evidence. Through the review of information provided to ONR, the Step 4 process should confirm that Hitachi-GE:

   - has properly justified the higher-level claims and arguments;
   - has progressed the resolution of issues identified during Step 3; and
   - has provided sufficient detailed information to allow ONR to come to a judgment of whether a DAC can be issued.

4. During this Control and Instrumentation (C&I) GDA Step 4 assessment I have undertaken a detailed assessment, on a sampling basis, of the safety and security case evidence. The full range of items that might form part of the assessment is provided in ONR's GDA Guidance to Requesting Parties (Ref. 1). These include:

   - consideration of issues identified in Step 3;
   - judging the design against the Safety Assessment Principles (SAPs, Ref. 4) and whether the proposed design reduces risks to ALARP;
   - reviewing details of the Hitachi-GE design controls, procurement and quality control arrangements to secure compliance with the design intent;
   - establishing whether the system performance, safety categorisation and classification, and reliability requirements are substantiated by the engineering design;
   - assessing arrangements for ensuring and assuring that safety claims and assumptions are realised in the final as-built design; and
   - resolution of identified nuclear safety and security issues, or identifying paths for resolution.

5. This is my report from the ONR's Step 4 assessment of the Hitachi-GE's UK ABWR design in the area of C&I.

## 1.2 Scope

6. The scope of my assessment is described in my Step 4 C&I assessment plan (Ref. 12), and has centred primarily on the C&I associated with main reactor systems, covering C&I safety case argumentation, architecture, platforms, systems, and qualification of complex C&I components. My assessment has focussed on systems and equipment of the greatest importance to reactor risk, sampling as appropriate, and also considered technical novelty and the feasibility of proposed C&I designs.

7. It has not been my intent to assess all C&I for the UK ABWR, but to confirm, by appropriate sampling, that appropriate design principles have been established, that these meet regulatory expectations, and that these principles are reflected in the C&I designs presented during GDA.

8. During GDA, as part of their ALARP justification, Hitachi-GE undertook a review of the C&I provisions proposed for the UK ABWR. Hitachi-GE considered UK relevant good

practice and the technologies available for high integrity applications. As a result of this exercise, the UK ABWR C&I design proposed for the UK has a number of enhancements over the baseline design. The design documentation submitted by Hitachi-GE for assessment incorporated the design modifications proposed for the UK and the safety case described their safety impact (see e.g. the ALARP section in the Pre-Construction Safety Report (PCSR), Ref. 40)

9. During GDA, the C&I design submissions were safety case led and established the principles for detailed design which will be undertaken post-GDA. For this reason, the decision on adequacy for GDA is based on verification that the principles proposed for the main C&I systems are adequate. My expectation is that during the development of the detailed design, the licensee will confirm that the principles established in GDA are adequately implemented. ONR will seek confirmation of this as part of its normal regulatory interactions and permissioning activities.

10. The scope of my assessment is appropriate for GDA because the activities described above establish whether the overall C&I Safety Case meets ONR's expectations for GDA as expressed in relevant SAP's and TAG's, and that the C&I systems and equipment important to safety are feasible and capable of delivering the necessary risk reduction and functionality.

### 1.3 Method

11. My assessment complies with internal guidance on the mechanics of assessment within ONR (Ref. 3).

# 2 ASSESSMENT STRATEGY

## 2.1 Pre-Construction Safety Report (PCSR)

12. ONR's GDA Guidance to Requesting Parties (Ref. 10) states that the information required for GDA may be in the form of a PCSR.

13. Technical Assessment Guide (TAG) 051 sets out regulatory expectations for a PCSR (Ref. 8). Further information relating to my assessment of the PCSR and referenced documents is given in section 4 of this report.

## 2.2 Standards and criteria

14. The standards and criteria adopted within this assessment are principally ONR's Safety Assessment Principles (SAPs) (Ref. 4), internal TAGs (Refs. 5, 6, 7, 8 and 9), relevant national and international standards and relevant good practice informed from existing practices adopted on UK nuclear licensed sites.

### 2.2.1 Safety Assessment Principles

15. The key SAPs applied within my assessment are listed in Annex 1. Of those listed, I have focussed on SAPs of particular relevance to the C&I design during GDA, including safety requirements identification (e.g. EKP.4, ECS.1, ECS.2, EMT.6, EHA.10, ESS.2), C&I architectural arrangement (e.g. EKP.3, EDR.2, EDR.3, ESS.1), C&I platform design (e.g. ECS.3, ECS.4, ESS.15, ESS.21, ESS.27), and C&I systems' capability (e.g. EDR.1, EDR.4, ERL.2, ESS.7, ESS.8, ESS.17, ESS.19, ESS.20, ESS.21, ESS.22, ESS.26).

### 2.2.2 Technical Assessment Guides

16. The TAGs that I have used to inform my assessment are set out in Annex 2.

### 2.2.3 National and international standards and guidance

17. International standards and guidance that have I have referenced are set out in Annex 3.

## 2.3 Use of Technical Support Contractors (TSCs)

18. It is common for ONR to use TSCs during GDA, for example to provide additional capacity for submission reviews, to enable access to independent advice and experience, to utilise specialist knowledge of analysis techniques and models, or to enable ONR's inspectors to focus on effective regulatory decision making.

19. The process used by ONR to select the TSC for the UK ABWR Step 4 GDA C&I work was competitive and included consideration of technical capability, capacity, understanding of GDA objectives and ONR regulatory processes, and cost effectiveness.

20. All technical reviews of UK ABWR documentation were conducted under the direction of, and supervision by, ONR. ONR worked in parallel with TSC reviewers, assessing the C&I safety case (including areas not explicitly covered by the TSC) but ensuring activities remained coordinated where necessary.

21. ONR arranged for the TSC to attend face-to-face meetings with Hitachi-GE to facilitate the effective and efficient exchange of information, and to allow the TSC to ask specific and detailed questions of Hitachi-GE subject matter experts, both in the UK and Japan. ONR was present at all interactions between the TSC and Hitachi-GE. Other than these interactions, the TSC did not communicate directly with Hitachi-GE.

22. Regulatory judgement on the adequacy or otherwise of the UK ABWR C&I design and safety case was made exclusively by ONR. ONR raised, managed, and closed, as appropriate, all ROs and RQs and meeting actions with Hitachi-GE.

23. The scope of work undertaken by the TSC included:

- reviews of the evidence made available to answer Technical Observations (TO's) raised by previous TSC reviews during Step 3, and documented in reports (Refs. 132, 133);
- a sample-based review of the evidence submitted by Hitachi-GE to identify how ONR SAP's relating to C&I have been satisfied;
- a sample-based review of the evidence submitted by Hitachi-GE to demonstrate that the main design and implementation standards relevant for the C&I systems and equipment have been selected, and complied with;
- sampling of the detailed design and implementation evidence of the Class 1, 2 and 3 platforms;
- sampling of the detailed evidence of the implementation methods for Class 1 systems, Class 2 systems, and relevant aspects of Class 3 systems;
- sampling of the detailed evidence of C&I architecture safety capability, including a review of the overall system integration;
- sampling of the detailed evidence of the diversity of the designs of platforms and systems contributing to the implementation of safety functions, and review of the possible contribution of platforms and systems to common cause failure; and
- review of submissions made by Hitachi-GE in response to RO's, in accordance with the resolution plan programme (although ONR made all decisions regarding closure of RO's).

24. ONR strategically selected the work to be undertaken by the TSC, taking into account technical requirements, capabilities, and timings of Hitachi-GE submissions. ONR developed a specification for their work, and provided further guidance where necessary, ensuring that work was correctly targeted and of a suitable standard. ONR recognised the potential for TSC independence to be compromised by these activities, and took steps to avoid this, regularly confirming that the TSC remained satisfied that ONR oversight was appropriate.

25. ONR regularly reviewed the outcome of the TSC activities, confirming their understanding of observations, and where necessary requesting additional depth of review.

26. Table 1 sets out the broad areas where I used the TSC during GDA Step 4 C&I assessment.

| Work Package | Review area identifier |
|---|---|
| Structure and clarity of the C&I safety case | RA.1 |
| Evidence of adequacy of C&I architecture | RA.2 |
| Confirmation of the adequacy of the platforms | RA.3 |
| Confirmation of the adequacy of the systems | RA.4 |
| Adequacy of the Human Machine Interfaces | RA.5 |

**Table 1.** Work packages undertaken by the technical support contractor.

27. The TSC produced reports (Refs. 32-36) that addressed the scope of work listed above, and responses to RQs and meeting actions placed on Hitachi-GE. The TSC

reports in Refs. 32-36 include a summary statement of the results of its work and observations. Observations were made at two levels:

- A TO1 is considered by the TSC to be of sufficient importance that, if not adequately addressed during GDA, has the potential to result in a GDA Issue; a TO1 is more significant than TO2.
- A TO2 is less significant than a TO1 and necessary to complete the technical review, but on its own, is not of sufficient importance to result in a GDA Issue.

28. No observations at TO1 remain open at the end of GDA Step 4.

29. I have reviewed the TO2s raised by the TSC and, through a documented sentencing process (Ref. 114), as appropriate, incorporated these into Assessment Findings (see Annex 5). Where appropriate, the TSC TO2s provide further guidance on the source of GDA Assessment Findings.

30. I have incorporated the outcome of the work of the TSC in appropriate sections of this report, and commented on the relevance of findings, as appropriate, on the outcome of my assessment.

### 2.4 Interaction with other technical assessment topic areas

31. GDA requires the submission of an adequate, coherent and holistic generic safety case. Regulatory assessment cannot therefore generally be carried out in one isolated topic area as safety issues are often of a multi-topic or cross-cutting nature.

32. As a consequence, during my GDA Step 4 assessment I have led and participated in many interactions with ONR inspectors in other topic areas. Interactions have been conducted in a number of different ways, including internal ONR meetings and meetings with Hitachi-GE, face-to-face, by teleconference, or by video conference, as appropriate.

33. For each cross-cutting topic in the C&I area I identified those technical areas contributing to safety or security and facilitated adequate participation and consensus in interactions to ensure sound assessments were achieved.

34. Examples of interactions with other technical areas are given in the table below:

| Cross cutting topic | Discipline | Examples of interactions |
|---|---|---|
| Categorisation of safety functions and Classification of systems | FS, PSA | • Assignment of classification and categorisation of safety functions according to fault studies analysis<br>• Classification of the PCntlS. |
| Reliability of C&I systems | PSA, ME, EE | • PSA modelling of the reliability for C&I components for the adequacy of different classification of C&I systems<br>• heating, ventilation and air conditioning (HVAC) provision and availability for the C&I systems<br>• Provision and availability of power supply (main, essential, emergency and backup) |
| Provision of Backup Building | PSA, SA, EE | • Provision of safety case for the SA C&I system and availability of power supply (i.e. main, backup and emergency) |

| | | |
|---|---|---|
| | | • Risks arising from C&I equipment |
| Exceptions to segregation | IH, EE | • Segregation requirements<br>• Avoidance of CCF. |
| Design of HMI | HF | • HMI requirements<br>• Alarm design |
| Smart device identification and qualification | ME, EE | • Identification of smart devices in embedded equipment<br>• Avoidance of smart devices in the backup support systems |
| RPV Instrumentation sensing lines | PSA, SI, IH, FS | • Common use of RPV instrumentation sensing lines. |
| Testing and Maintenance | FS, PSA, ME, EE, HF | • Testing and maintenance methodology.<br>• Testing and maintenance intervals |
| Lightning and EMI | IH, EH, EE | • Lightning design basis<br>• Methodology for management of EMI including cable routing and installation |
| Spent Fuel Route | IH, FS, ME, EE, NL | • Safety case for spent fuel route;<br>• Reactor Building Overhead Crane C&I |
| Fuel failures and control rod movement faults | FS, FC | • Neutron monitoring system calibration<br>• Control rod movement faults |
| Lighting and Communications | EE, HF | • Categorisation and classification of lighting and communication functions and systems. |
| C&I system control transfer | IH, HF | • C&I system control transfer via transfer switches |
| Cyber security | CNS | • Resistance to Cyber attack<br>• Safety contribution of security systems |
| Radioactive waste and decommissioning | FS, NL | • Leak detection system<br>• Reactor vessel instrumentation testing |

**Table 2.** Examples of C&I interactions with other topic areas

35. As necessary, these interactions have been recorded in ONR's document management system (TRIM), and only those appropriate for the purposes of recording the outcome of the Step 4 C&I assessment have been included in this report.

### 2.5 Sampling strategy

36. It is seldom possible, or necessary, to assess a safety case in its entirety, therefore sampling is used to limit the areas scrutinised, and to improve the overall efficiency of the assessment process. Sampling is done in a focused, targeted and structured manner with a view to revealing any topic-specific, or generic, weaknesses in the safety case.

37. My sampling strategy for this assessment concentrated on the adequacy of the C&I safety case, establishing key principles relating to the C&I architecture, platforms and systems important to safety, and confirming that these have been met in the design, with a focus on:

- Safety case structure, clarity and linkage (e.g. safety property claim accuracy).
- C&I architecture (e.g. separation of systems of different safety classes).
- Platforms and systems of a greater safety significance and/or novelty (e.g. Class 1 platform and systems).
- Regulatory observations raised during previous steps of GDA (e.g. testing and maintenance).
- Emerging findings during the ongoing assessment (e.g. future plans for smart device qualification).

38. I consider this approach to be proportionate in ensuring that the outcome of my assessment meets the objectives of GDA.

39. Additional information about the scope of the assessment can be found in Section 1.2 and Section 2.6 of this report.

### 2.6 Out of scope items

40. As indicated in Section 1, the scope of this C&I assessment is broad, covering C&I systems directly associated with reactor operation and safety, as necessary. However, I have not assessed in detail those C&I systems whose design is dependent on site configuration and licensee preferences (e.g. alarm systems). Similarly, I have not assessed C&I components that were excluded from GDA (e.g. those sensors and actuators that were out of scope).

41. My assessment of the fuel route includes cask handling operations within the reactor building. I note that operational requirements for the cask handling operations have not been identified during GDA, and so my assessment has been limited to the feasibility of the C&I designs, as detailed design will be completed post-GDA. However, fuel handling operations undertaken after the spent fuel has left the reactor building, including within the spent fuel interim store, are out of scope.

42. Whilst I have considered likely operating regimes and measures to be deployed during emergencies in my assessment of C&I systems, detailed information on these is not available during GDA and so I have not assessed technical specifications, operating procedures or emergency arrangements in detail.

## 3 REQUESTING PARTY SAFETY CASE

44. The documentation structure for the safety justification of the UK ABWR C&I systems comprises of three main tiers (Ref. 39), i.e.:

- tier-1: PCSR Chapter 14 (Ref. 39), providing a high level description of the C&I proposed for the UK ABWR;
- tier-2: Overall BSC justifying the C&I architecture (Ref. 44), supported by BSCs for each of the principal C&I systems important to safety (Ref. 45-51); and
- tier-3: Technical reports on platform justifications (e.g. Ref. 56) and other specific topics (e.g. smart devices in Refs. 67-69).

Supporting documents, such as system design description (SDDs), interlock block diagrams (IBDs), failure mode and effect analyses (FMEAs), were also provided. Figure 1 gives an example of the relationship between the main submissions in the C&I safety case and the supporting documents.

45. The main C&I systems provided in the UK ABWR are described in (Ref. 44) and include:

- a control system for the normal operation of the plant (including PCntlS, ACS and PCS);
- a primary protection system (SSLC) delivering Category A safety functions, complemented by a separate system (SACS) delivering Category B and C safety functions that support SSLC functions or are used after the SSLC initiates safety-protection operations;
- a secondary protection system (HWBS) to manage frequent design basis faults together with additional common cause failure of the SSLC;
- a dedicated severe accident C&I system to manage all classes of severe accidents defined in section 26.4 of Chapter 26 of the UK ABWR PCSR.

46. The documentation structure for the human machine interface (HMI) consists of (Ref. 39):

- tier-1: PCSR Chapter 21 (Ref. 41), providing a high level justification of the adequacy of the HMI provisions in the UK ABWR and considering the inputs from PCSR Chapter 27 on human factors (Ref. 75) and PCSR Chapter 14 on C&I (Ref. 39);
- tier-2: BSC justifying the overall HMI provisions (Ref. 52), supported by BSCs for each of the principal HMIs (Refs. 53-55);
- tier-3: Other supporting documents, e.g. TR related to strategy for HMI utilisation, human reliability, and C&I design.

Figure 2 provides an example of the relationship between the main submissions in the HMI safety case and the supporting documents.

47. Further documentation on C&I systems important to safety or associated with essential services that perform a range of functions referenced from the overall BSC on architecture (Ref. 44) was submitted during GDA Step 4, including Basis of Safety Cases on Radioactive Waste, Electrical system, Standby Liquid Control System, Control Rod Drive System, Heating Ventilation and Air Conditioning System, Fuel Handling machine and Reactor Building Overhead Crane.

48. To inform the content and consistency of the UK ABWR safety cases, Hitachi-GE produced a safety case development manual (Ref. 38) containing cross-discipline guidance describing how to:

- structure the documentation in the safety case;

- approach the safety categorisation of the functions and classification of the systems;
- use CAE to organise the safety case and provide adequate evidence supporting the justification;
- develop an approach to reduce the risk ALARP, as required in the UK nuclear regulatory context.

49. The C&I safety case uses a claims, argument and evidence (CAE) format. High level claims are identified at the PCSR level and justified through lower tier documentation, with argument and evidence as appropriate. When evidence is not available due to the limited design maturity of the systems during GDA, the documentation identifies gaps which will need to be addressed post-GDA.

50. In the C&I safety documentation, e.g. the PCSR (Refs. 39, 41) and BSC's (e.g. Refs. 44-55), the fundamental properties of the UK ABWR C&I systems are identified through safety property claims (SPCs) and safety functional claims (SFCs):

- SPCs define the main attributes of the systems in terms of non-functional properties. These were determined by Hitachi-GE subject matter experts, utilising expertise of ABWR design, experience of operation, and key national and international standards.
- SFCs define the functions that need to be delivered by each individual C&I system and are directly derived primarily from the fault schedules (e.g. Refs. 42, 43).

51. The Topic Report on Fault Assessment (Refs. 42, 43) provides, for each of the initiating events, the primary and secondary lines of protection, clarifying their actuation basis (i.e. automatic or manual), their categorisation/classification, and their relation with high level safety functions (HLSFs). Through the PCSR Chapter 14 (Ref. 39), the link between the HLSFs and the SFCs is established, ensuring that there is a direct flow of requirements from the fault schedule to the C&I system design documentation.

52. SPCs and SFCs are used throughout the C&I safety case, and justification that these have been satisfied uses a claims, argument and evidence approach. Depending on the claim, various sub-claims are derived from the main SPC/SFC or a single sub-claim is substantiated through multiple arguments.

53. An important aspect of the safety demonstration is the classification of safety systems and the application of appropriate design standards. Accepted practice is that the requirements of standards are more onerous for those systems that are more important to safety (i.e. Class 1 systems are implemented using safety standards applicable to Class 1 safety systems). In the UK, the importance to safety is typically judged by a combination of deterministic (e.g. the function performed by the system such as to shut down the reactor) and probabilistic (e.g. the reliability required of the system) criteria. For the UK ABWR, the SCDM in Ref. 38 identifies three safety Categories (namely A, B and C) and three safety Classes (namely 1, 2 and 3) as expected in SAP ECS.1/ECS.2 and in IEC 61226/IEC 61513.

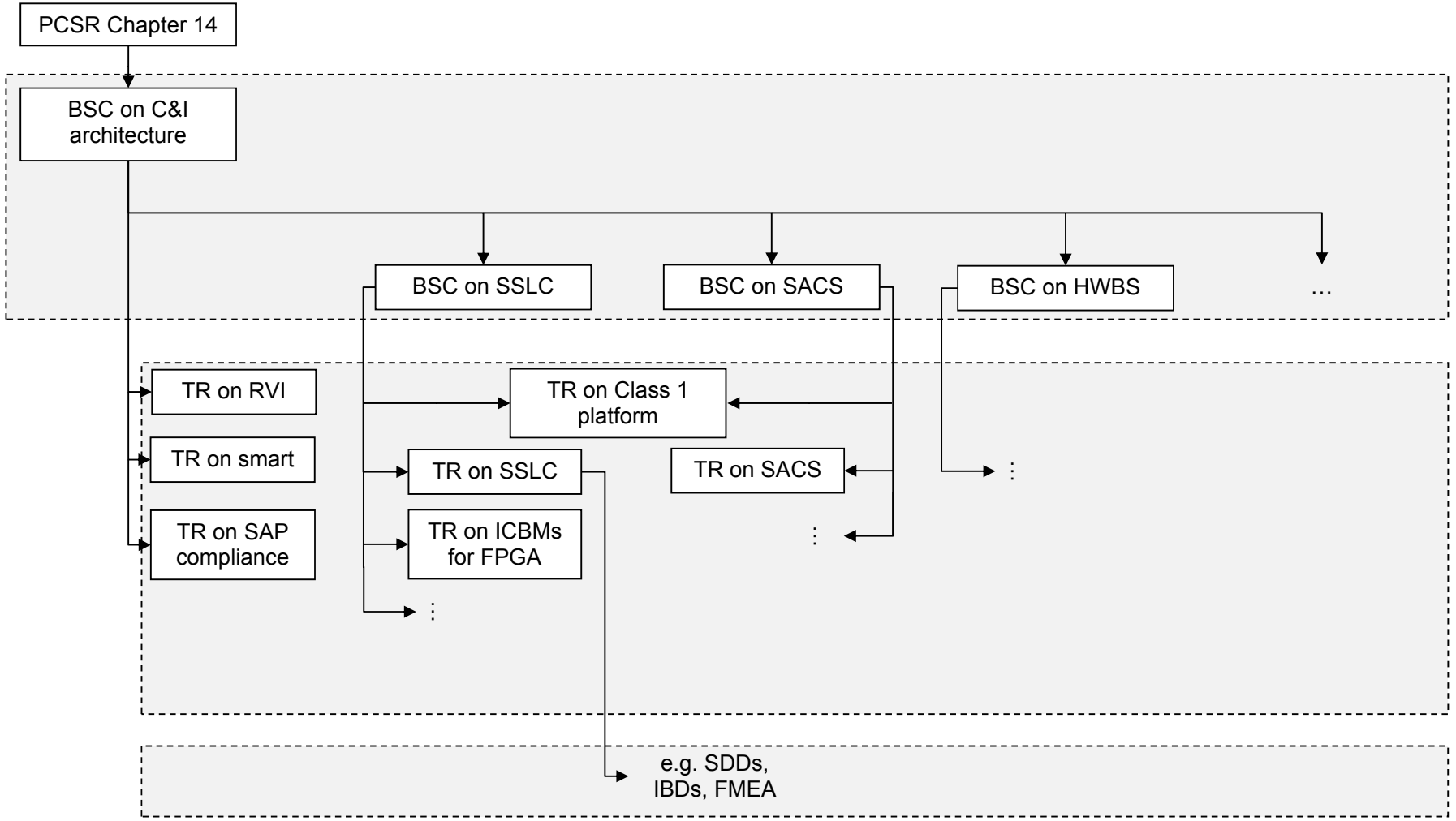


**Figure 1.** Example documentation structure (referred to as the C&I safety case) for the substantiation of the UK ABWR C&I architecture and systems.

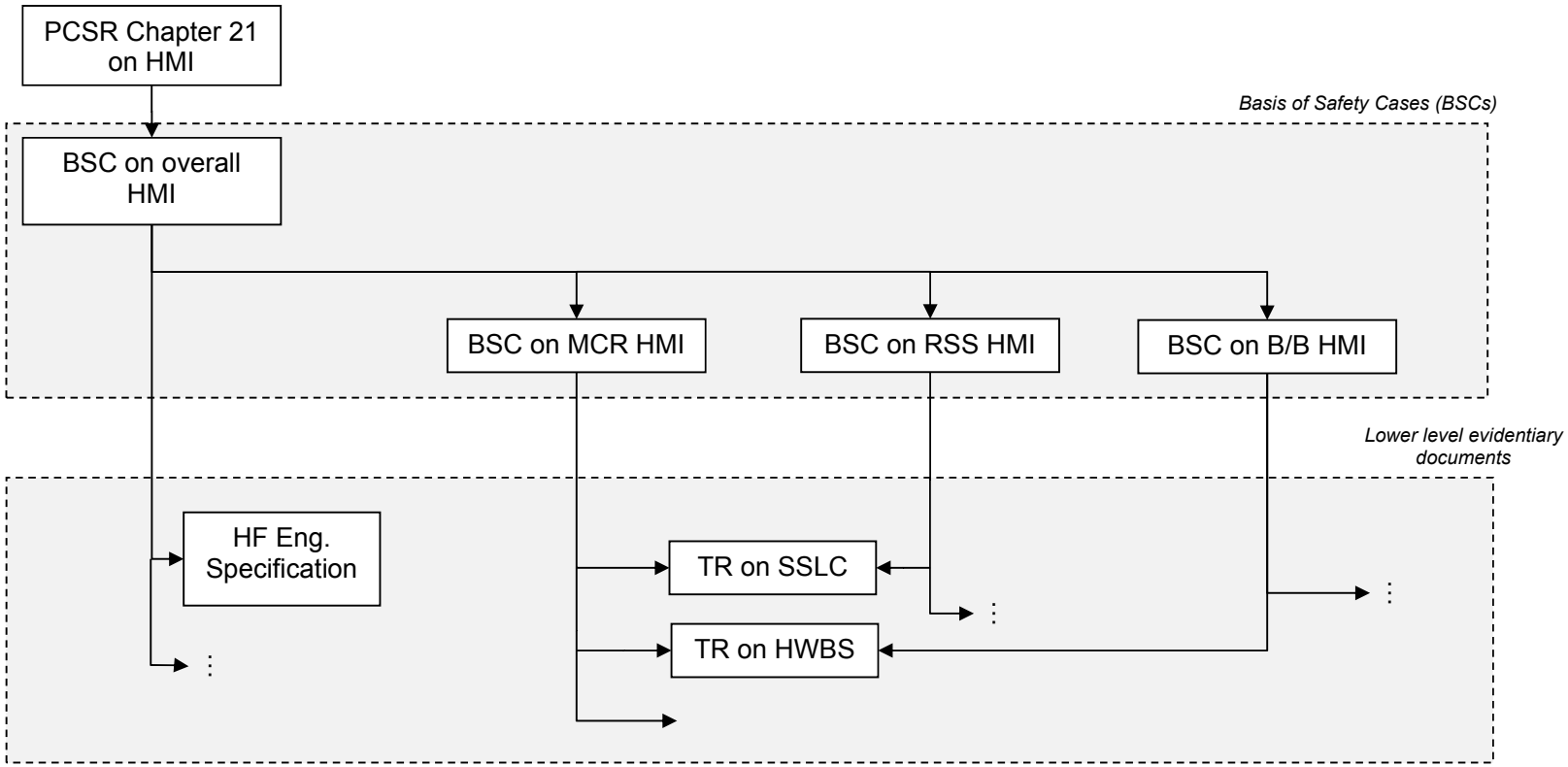


**Figure 2.** Example documentation structure (referred to as the HMI safety case) for the substantiation of the UK ABWR HMI architecture and systems.

# 4 ONR STEP 4 ASSESSMENT

54. This assessment has been carried out in accordance with ONR internal guidance on the “Purpose and Scope of Permissioning” (Ref. 11).

## 4.1 Scope of Assessment Undertaken

55. The scope of the Step 4 assessment of the C&I aspects of the UK ABWR was informed by the objectives of GDA (e.g. Ref. 1), the findings of earlier GDA steps (e.g. Refs. 2, 13), assessment plans (e.g. Ref. 12), and emerging findings in the C&I and other technical areas.

56. A number of C&I Regulatory Observations (ROs) were raised during earlier steps of GDA (Ref. 13) in a number of specific areas, including the Backup Building C&I, Hardwired Backup System, Class 1 HMI, the qualification of smart devices, protection system architecture, design substantiation of reactor vessel instrumentation, and testing and maintenance. My assessment has covered these areas and ROs.

57. Detailed design of aspects of the C&I of the UK ABWR have not been completed within the duration of GDA. However, detailed design information is not necessary for the successful completion of GDA, and therefore my assessment has focussed on confirming that the safety case and design principles established by Hitachi-GE for C&I systems important to safety meets ONR’s regulatory expectations and that there is adequate evidence these have been applied appropriately in the outline design.

## 4.2 Assessment

58. The following sections describe the general areas that I have assessed during GDA Step 4, covering the C&I safety case (see Figure 1), C&I architecture, C&I platforms, C&I systems, and other equipment utilising C&I components.

### 4.2.1 Safety case

59. As outlined in Section 3 of this report, Hitachi-GE delivered the C&I safety case (see Figure 1) for the UK ABWR through a structured set of submissions, with the PCSR being at the top and a series of BSCs, lower level topic reports, and evidence documents to support claims, arguments and evidence. Whilst PSCR Chapter 14 (Ref. 39) is the cornerstone for the C&I safety case, other chapters of the PCSR are particularly relevant to C&I, such as:

- PCSR Chapter 5 (Ref. 40) which includes information on the approach to categorisation/classification, and testing and maintenance; and
- PCSR Chapter 21 (Ref. 41) on HMI.

60. Hitachi-GE identified the main C&I claims in GDA Step 2, and defined the supporting arguments in GDA Step 3. In GDA Step 4 my expectation was that Hitachi-GE demonstrates that C&I claims have been satisfied by the arguments and evidence provided, noting that detailed design is not complete.

61. In my assessment of the overall C&I safety case, I have benchmarked Hitachi-GE submissions against key points in NS-TAST-GD-051 (Ref. 8) , e.g. requiring that:

- all references and supporting information should be identified and be easily accessible;
- there should be a clear trail from claims through the arguments to the evidence that fully supports the conclusions, together with commitments to any future actions;

- a safety case should accurately represent the current status of the facility in all physical, operational and managerial aspects;
- for new facilities or modifications, the safety case should accurately represent the design intent;
- there should be reference from the safety case to important supporting work, such as engineering substantiation; and
- the safety case should be able to act as an entry point for accessing all relevant supporting information on which it is built.

62. At the structural level, I found that the approach taken by Hitachi-GE to present the C&I safety case was adequate for GDA, because the rationale of the safety case is sufficiently clear, it is easy to navigate through the documentation (e.g. Figure 1 and 2 in this report), and the substantiation using a CAE structure is adequately developed for this stage of the project (e.g. review in Ref. 32). In my assessment of the UK ABWR C&I safety case, I am satisfied that Hitachi-GE followed the approach outlined in the safety case development manual (Ref. 38), which promotes consistency between different technical disciplines and is effective in generating a clear and complete safety case for the UK ABWR.

63. In developing the design attributes for the UK ABWR C&I architecture and systems, Hitachi-GE adopted various levels of cross referencing of the SFCs and SPCs, characterising the functional and non-functional requirements. Specifically:

- HLSFs are identified in the Fault Schedule (Refs. 42, 43) and mapped through to the SFCs in the PCSR Chapter 14 (Ref. 39);
- a set of fundamental SPCs (i.e. SPC 1 to 9) are identified at the PCSR level (Ref. 39) and detailed for the various C&I systems to characterise their specific attributes, defining sub-claims in the relevant BSCs; and
- where appropriate, the evidence in lower tier documents (e.g. topic reports) is referenced back to the relevant SPCs it is supporting.

64. In my assessment, I found that this approach ensures an adequate level of traceability across the whole C&I documentation and constitutes an adequate basis for the development of the licensing documentation in future phases of the development of the UK ABWR.

65. I note that additional information relevant for the requirements capture has been identified within GDA in the form of assumptions and captured in the Hitachi-GE assumption management database (Ref. 76), which I consider good practice in ensuring the continuity of the project from GDA into licensing. Additionally, examples provided for the requirements capture for platforms (e.g. for Class 1 in Ref. 56) provides sufficient confidence that Hitachi-GE has adequate resources and tools available to support a future licensee in these activities post GDA.

66. I am also satisfied with the plan proposed by Hitachi-GE in Ref. 38 to develop post-GDA an engineering schedule, to link the fault schedule to the engineering substantiation of the systems requirements, specified by a combination of the SFCs and SPCs. My expectation is that, as part of the normal development of the safety case, the licensee will ensure that the safety case development methodology used during GDA is deployed for the further definition of the functional and non-functional requirements for the UK ABWR C&I systems important to safety.

67. An important part of the verification of the suitability of the C&I design proposed for the UK ABWR is verification that it recognises the expectations described in ONR SAPs and requirements in international standards relevant to the UK nuclear industry. In this respect, Hitachi-GE produced a document (Ref. 57) that documented an internal assessment of whether principles in the applicable C&I SAPs are satisfied by the proposed C&I architecture and systems. This uses a CAE format and highlights the

instances where future evidence will need to be developed post GDA as part of the detailed design. I found that the approach taken in Ref. 57 was an effective way for Hitachi-GE to confirm that the design proposed for the UK ABWR C&I is in line with ONR SAPs relating to C&I.

68. Although my assessment considered the information provided in Ref. 57, I carried out an independent assessment of the C&I design against the relevant SAPs, mainly starting from the PCSR C&I Chapter (Ref. 39) and the BSCs (Refs. 44-51), including (see Annex 1 for a full list):

- safety requirements identification and categorisation and classification (e.g. EKP.4, ECS.1, ECS.2, EMT.6, EHA.10, ESS.2);
- C&I architectural arrangement (e.g. EKP.3, EDR.2, EDR.3, ESS.1);
- C&I platform design (e.g. ECS.3, ECS.4, ESS.15, ESS.21, ESS.27);
- C&I systems' capability (e.g. EDR.1, EDR.4, ERL.2, ESS.7, ESS.8, ESS.17, ESS.19, ESS.20, ESS.21, ESS.22, ESS.26).

69. Based on the detailed assessment in Refs. 23-36, I judge that the architecture and the design of the C&I proposed for the UK ABWR adequately considers UK regulatory expectations. My expectation is that future assessment activities by ONR post-GDA shall confirm this at the detailed design level. Additional details related to the assessment of the adequacy of the design against ONR SAPs relating to C&I are presented in following sections of this report.

70. I verified in the PCSR (Ref. 39) and in the relevant BSCs (Refs. 44-51) that Hitachi-GE has considered the relevant C&I standards for nuclear installations applicable in the UK and am satisfied that key standards are utilised for the development of the C&I systems for the UK ABWR (including the IEC SC 45A series).

71. I sampled submissions to ensure that the key clauses in the relevant international standards are considered in the design of the UK ABWR C&I architecture and systems (see details of the assessment sampling in Refs. 32-36). I raised RQ-ABWR-1422 to clarify the approach proposed by Hitachi-GE to demonstrate the full coverage of the expectation in relevant standards. In response to this RQ, Hitachi-GE presented a suitable approach to provide an explicit clause-by-clause compliance against key IEC standards and provided examples of its application for the main systems against the key standards (e.g. see the SSLC the compliance statement against IEC 62566 and IEC 61513 in Refs. 56 and 58).

72. My expectation is that the exercise will be completed post-GDA to take into account detailed design information and ensure the design proposed for the UK ABWR C&I meets the requirements of the key nuclear standards. I therefore raise an assessment finding for the licensee to complete the compliance analyses against key nuclear standards, e.g. those listed in Annex 3 of this report, justifying if necessary whether any clause in the standards is considered not applicable (see point (a) of AF-UKABWR-CI-001 below).

73. In my assessment of the C&I safety case for the UK ABWR, I raised RQ-ABWR-1439 (Ref. 37) to clarify the origin of the SPCs. Hitachi-GE's response (Ref. 59), explained that these were derived by Japanese subject matter experts, considering relevant standards (both national and international) and their experience in the reference design. I found that the SPCs and related sub-claims provided by Hitachi-GE for the UK ABWR are sufficiently developed for GDA and represent an adequate basis for the future detailed design activities in licensing. My expectation post-GDA is that the SPCs will be further analysed and consolidated. This activity should be informed, for example, by the consolidation of the site specific engineering principles and should also consider any gaps identified from the compliance assessment against the relevant

nuclear standards. I therefore raise an assessment finding for the licensee to verify the completeness of safety property claims and sub-claims (see point (b) below).

> *GDA Assessment Finding:* ***AF-UKABWR-CI-001*** *- During GDA, Hitachi-GE has demonstrated to ONR's satisfaction that the key principles in the relevant nuclear standards are considered in the UK ABWR C&I design and safety case. Post GDA, ONR's expectation is for this exercise to be extended to all of the relevant C&I systems that were out of scope of GDA, and to further develop the work by considering the detailed design information and, if necessary, justifying whether any clause in the standards is considered not applicable. The expectation is that this should be carried out as part of the consolidation of the system attributes (i.e. the safety property claims in Hitachi-GE nomenclature) identified in the UK ABWR C&I safety case.*
>
> *The licensee shall:*
> *a. Produce a demonstration of compliance to relevant international nuclear sector C&I standards, for UK ABWR C&I systems and for the overall architecture as appropriate.*
> *b. Develop an appropriate methodology to identify any potential gaps in the safety property claims, and apply this across the C&I systems in the UK ABWR architecture.*
>
> *For further guidance see the Technical Observations for AF-UKABWR-CI-001 in Annex 5.*

74. My assessment of the BSC for the SSLC (Ref. 45) identified that in several instances the CAE referred to the Class 1 platform report (Ref. 80) as evidence to justify claims related to the whole system (see examples in Ref. 34). Until the final SSLC system requirements specifications have been confirmed during detailed design it will not be possible to confirm that the substantiation at platform level is adequate for the system level (including the application). I find that a more detailed justification will be necessary post-GDA, when its detailed design is further developed, to ensure that the substantiation made at platform level is fully applicable at the SSLC system level (including the application), e.g. considering the suitability of the techniques and measures and of the verification and validation. For this purpose, I raise an assessment finding for a future licensee to use the detailed design to complete the development of the evidence that the SSLC platform supports system level claims.

> *GDA Assessment Finding:* ***AF-UKABWR-CI-003*** *- During GDA, Hitachi-GE provided adequate submissions regarding the suitability of the vCOSS®/NCFS-1 platform for use at safety class 1. In the safety case provided in GDA, in several instances Hitachi-GE referred to the evidence relating to the safety class 1 platform for the whole SSLC system (including the application). Until the final SSLC system requirement specifications have been fully determined during detailed design, it will not be possible to confirm that the substantiation at platform level is adequate at the system level.*
>
> *The licensee shall assess and adequately report on the suitability of proposed class 1 platform to support the system level requirements for the SSLC.*
>
> *For further guidance see the Technical Observations for AF-UKABWR-CI-003 in Annex 5.*

75. As part of the assessment of the C&I safety case, the C&I TSC identified a number of technical observations (Refs. 32-36). I raised with Hitachi-GE (via RQs (Ref. 37) or in meetings) only those observations which I found relevant for this stage of the project,

considering the design maturity expected for GDA. Hitachi-GE satisfactorily responded to these challenges, updating the documentation as appropriate.

76. I considered a number of other observations identified in Refs. 32-36 not to be a priority for the purposes of GDA. I therefore did not raise them with Hitachi-GE within GDA Step 4 in order to focus effort on the matters most relevant to nuclear safety at this stage of the project (see e.g. Section 1.2 in this report). These observations are nevertheless important to future phases of the UK ABWR development, as they cover areas such as:

- inconsistencies across the safety case submissions;
- limitations in the justification of claims in the C&I safety case documentation; and
- evidence needed in the CAE, but not identified by Hitachi-GE as necessary to be developed during GDA.

77. As described in NS-TAST-GD-051 (Ref. 8), ONR's expectation is that the safety case represents an accurate reflection of the C&I design and that the safety justification is sufficiently clear and supported by evidence. I therefore raise an assessment finding for the licensee to review the technical observations identified during GDA Step 4, develop a strategy for their consideration as part of the further development of the C&I safety case for the UK ABWR, and clarify the arrangements in place going forward to ensure an adequate level of oversight and ownership of the final safety case.

> *GDA Assessment Finding:* ***AF-UKABWR-CI-002*** *- During GDA, a number of observations relating to the C&I safety case were identified in the C&I assessment. These are not considered to present an impediment to the closure of GDA, but they should be reviewed, and as appropriate, taken into account in detailed design and site-specific safety case development work post-GDA. Because these observations resulted from a sampling of the safety submissions, ONR's expectation is that they should be addressed considering the wider implication on the C&I documentation and that suitable arrangements are put in place to ensure the clarity and consistency of future revisions of the C&I safety case*
>
> *The licensee shall:*
>
> *a. Develop a strategy for the resolution of the technical observations made in GDA Step 4 as part of the further development of the C&I safety case for the UK ABWR.*
>
> *For further guidance see the Technical Observations for AF-UKABWR-CI-002 in Annex 5.*

78. Overall, I judge the C&I safety case to be sufficiently well developed for the purposes of GDA, with an appropriate structure and level of detail.

### 4.2.2 C&I architecture

79. During GDA Step 3, high level assessment of the UK ABWR C&I architecture was undertaken. Further review of the C&I system level architecture has been undertaken during GDA Step 4, with a review of the evidence presented by Hitachi-GE that supports the architecture related claims and arguments presented in the PCSR, and identified references.

80. The objective of my C&I system level architecture assessment in GDA Step 4 was to consider the overall C&I architecture, looking at safety design principles in the Hitachi-GE submissions, namely:

- defence-in-depth and failure mode considerations, including CCF;
- independence, separation, segregation and diversity;
- provision for automatic and manual safety actuation;
- appropriateness of equipment type and Class; and
- interconnection between different C&I systems.

81. The overall architecture of the UK ABWR C&I is presented in the PCSR (Ref. 39) and its justification is provided in the architecture BSC (Ref. 42). The C&I system level architecture comprises:

- a primary protection system, the SSLC;
- a secondary protection system, the HWBS;
- a non-essential support system for the SSLC, i.e. the SACS;
- a system dedicated to the management of severe accidents, i.e. SA C&I;
- several C&I systems are dedicated to the operating functions of the UK ABWR, namely the PCntlS, the PCS and the ACS; and
- HMI interfaces for the operator monitoring and control (see description in section 4.2.6).

82. Table 3 below lists each C&I system, the plant status for which it is claimed, and provides information relevant to its safety Class, Category of the safety function(s) that it implements and reliability target. It is noted that numerical plant safety targets are not required to be demonstrated for the PCS and SA C&I systems, therefore no specific target is set for these systems except for the part of SA C&I system shared with the HWBS which has the same reliability targets of the HWBS to ensure the SA C&I does not impede the delivery of a HWBS safety function.

| Plant status | System | Safety Function Category | Safety Class | Reliability target |
|---|---|---|---|---|
| Normal condition | Plant Control System (PCntlS) | - | 3 | pfd: n.a.<br>ffpy: $10^{-1}$/y |
| | Reactor/Turbine Auxiliary Control System (ACS) | - | 3 | pfd: n.a.<br>ffpy: $10^{-1}$/y |
| | Plant Computer System (PCS) | - | 3 | pfd: n.a.<br>ffpy: n.a. |
| Fault condition | Safety System Logic and Control System (SSLC)<br>• Reactor Protection System<br>• Emergency Core Cooling System/<br>• Engineered Safety Features | A | 1 | pfd: $10^{-4}$<br>ffpy: $10^{-4}$/y |
| | Safety Auxiliary Control System (SACS) | B | 2 | pfd: $10^{-2}$<br>ffpy: $10^{-2}$/y |
| | Hardwired Backup System (HWBS) | A | 2 | pfd: $10^{-2}$<br>ffpy: $10^{-2}$/y |
| Severe accident | Severe Accident (SA C&I), principal role, or sharing with HWBS | B | 2 | pfd: n.a.<br>ffpy: $10^{-2}$/y |

| | | | | |
|---|---|---|---|---|
| | Severe Accident C&I (SA C&I), for backup role | B | 3 | pfd: n.a.<br>ffpy: n.a. |

**Table 3.** Main C&I systems for the UK ABWR.

83. In my assessment of the C&I architecture, I confirmed with Hitachi-GE that a failure of the SACS ("supporting system" to the SSLC, according to the nomenclature in Ref. 39) would not affect the functionality of the primary line of protection (i.e. SSLC). Ref. 60 confirmed this, clarifying the lower Category SACS safety functions had been removed from the SSLC to ensure they could not interfere with the Category A SSLC functions. I am content with the modified architecture because it ensures the lower category functions will not interfere with Category A safety functions.

84. As described in Refs. 38, 44 and 119, the approach to functional allocation to C&I system is directly derived from the fault schedule (Refs. 42, 43), which identifies the level of protection required against each initiating event (for the design basis and beyond design basis, covering appropriate hazards). For frequent faults, two independent lines of protection are identified in Refs. 42, 43, placing a requirement for diversity and segregation on the C&I systems delivering the related primary and secondary safety functions. C&I-initiated spurious actuations of the PCntlS are considered in the fault schedule (Refs. 42, 43), introducing an additional requirement of diversity between the PCntlS/ACS/PCS and the SSLC/HWBS. The UK ABWR design also provides a separate system to manage severe accidents (SAs). Overall, I am content with the Hitachi-GE allocation process for safety functions to C&I systems as it is in line with IEC 61226/IEC 61513/IAEA SSG-30. The full ONR assessment of the adequacy of the categorisation/classification of the safety function is provided in the fault studies area (Ref. 61).

85. With respect to the PCntlS, in the latter stages of GDA Step 4 Hitachi-GE notified ONR with Ref. 63 of a misalignment between the initial safety classification for the system (Class 2) and the result of the application of the principles established in the safety case development manual (Ref. 38). I raised RQ-ABWR-1011 and RQ-ABWR-1434 (Ref. 37) to seek clarity regarding the rationale behind the PCntlS safety classification as Class 3. In Refs. 64, 65, Hitachi-GE clarified that the PCntlS does not deliver any safety functions and is not credited either as primary or secondary means of protection in the fault schedule (Refs. 42, 43). For this reason, Hitachi-GE justified the classification of the PCntlS based on the direct classification principle in accordance with IAEA SSG-30.

86. Under this standard, a design provision (such as the PCntlS) can be directly classified "because the significance of its postulated failure fully defines its safety class without any need for detailed analysis of the category of the associated safety function" (IAEA SSG-30, para. 2.9). Based on para. 3.11 and 3.23 in IAEA SSG-30, the PCntlS can be classified as safety Class 3. Refs. 64, 65 also clarifies that, in the context of the overall UK ABWR safety case (Refs. 38 and 40), this classification is conservative as compared with IAEA SSG-30 and NS-TAST-GD-094 (Ref. 9) in that it allows safety Class 3 systems only where there are two independent layers of protection (i.e. a Class 1 and a diverse Class 2 system) against postulated spurious actuation of the lower class system.

87. I sought confirmation from the ONR FS inspector regarding the consideration of PCntlS spurious actuation in the fault schedule and it was confirmed in Ref. 16 that adequate coverage of spurious actuation faults from a deterministic point of view has been achieved considering the actuation of various PCntlS functions (one at a time, with conservative assumptions on the others). The ONR PSA inspector also confirmed that in Refs. 63, 64 PSA was used to risk-inform the decision to align the classification of PCntlS to the expectation in the SCDM (Ref. 38) and that the confirmation that the

PCntlS safety classification is Class 3 has limited impact due to the small number of claims made on the plant control system for the UK ABWR (Ref. 81).

88. On the basis of the Hitachi-GE responses to the RQs in Refs. 64, 65 and the ONR PSA/FS assessments (Refs. 81 and 61), I found the overall argument supporting the classification of the PCntlS as a Class 3 system to be acceptable. However, whilst the PCSR C&I chapter (Ref. 39) correctly reflects the argument in Ref. 65 about direct classification for the PCntlS, I identified some inconsistencies in the lower tier documents, which either state that the PCntlS delivers Category B safety functions (e.g. Ref. 49) or that its safety classification is Class 2 as assumed in earlier stages of GDA (e.g. Ref. 13). It is important for the overall safety case that the documentation reflects the actual design of the systems. I therefore raise an assessment finding for the future licensee to revise the C&I safety case and confirm that the safety classification of the PCntlS is properly and consistently incorporated throughout the suite of documents, providing an impact safety assessment where necessary (see point (a) of assessment finding AF-UKABWR-CI-004 below).

89. ONR raised RO-UKABWR-0007 earlier in GDA (Ref. 164) requesting analysis of spurious actuations arising from C&I systems. Hitachi-GE undertook analysis work and presented evidence during GDA step 4 that ONR considered sufficient to close this RO (assessment note, Ref. 165).

90. Subsequently my review of the C&I design and architecture of the PCntlS also identified the potential for common cause failures within the PCntlS to cause multiple spurious actuations (see details in Refs. 33 and 35). Because of the modest reliability claim for the PCntlS as a class 3 system (i.e. $10^{-1}$ ffpy), it is important to verify that PCntlS faults having the potential to result in more than one consequential spurious actuation are outside the design basis for the plant (e.g. ensuring that the PCntlS design and architecture provides adequate protection against their occurrence) or are adequately covered by safety analyses and by two layers of protection (i.e. a Class 1 and 2 systems, as claimed in Refs. 63-65 as part of the justification of the PCntlS safety classification).

91. I therefore raise an assessment finding for the future licensee to carry out a confirmatory analysis (see point (b) of assessment finding AF-UKABWR-CI-004 below). Additional guidance regarding multiple spurious actuations is available in Ref. 134.

> *GDA Assessment Finding: **AF-UKABWR-CI-004** - During GDA Step 4, Hitachi-GE provided a justification for the PCntlS being safety class 3 following a period earlier in GDA where inconsistent documentation implied the classification was safety class 2. This justification of the PCntlS as safety class 3, based on standards, deterministic and probabilistic arguments is considered acceptable for GDA. However, ONR's expectation post GDA is that further verification work is undertaken, based on the more detailed design information that will be available, to confirm that the PCntlS safety classification is correct and correctly reflected in the UK ABWR safety case.*
>
> *The licensee shall ensure consistency in the classification of the PCntlS and its justification throughout the whole safety case, including:*
> *a. A safety assessment of the impact of aligning the documentation of the PCntlS safety classification across all safety case documentation.*
> *b. A justification of the robustness of the PCntlS against faults which could cause spurious actuations, including multiple spurious actuations, considering:*
> - *The PCntlS architecture and data flow.*
> - *The effect of the use of multiple common components.*
> - *The measures deployed to manage the effects of failures.*

*For further guidance see the Technical Observations for AF-UKABWR-CI-004 in Annex 5.*

92. As clarified in Ref. 60, I note that prioritisation of actuators is not performed by C&I components. In general, separate actuators are controlled from different C&I layers of protection. I found this approach adequate because it minimises the number of interfaces between C&I systems of different safety classes and reduces the risk of a single point of C&I failure affecting the functionality of different layers of defence.

93. During my assessment I identified two exceptions to this. One exception is the control of the scram valves by both the SSLC and HWBS. In this case both the SSLC and HWBS are connected to separate pilot valves. This means the two C&I systems are not electrically connected and the lower class HWBS cannot influence the SSLC. Another exception is actuators controlled by both the HWBS and the SA C&I. In this case, the priority is not mediated by C&I systems but by the use of simple, manual transfer switches. I consider this to be adequate because the SA C&I cannot influence the HWBS except under severe accident conditions when the transfer switches have been used to activate the functions.

94. Following assessment of Hitachi-GE documentation, I raised RQ-ABWR-1422 (Ref. 37) to seek clarification regarding some of the key aspects of the C&I architecture (e.g. requirement specification, system classification, diversity). In my assessment of this RQ response (Ref. 60), I found that the C&I architecture proposed for the UK ABWR is broadly adequate with respect to the following:

- it provides an adequate level of defence-in-depth (i.e. different layers of protection are allocated to different systems);
- it makes acceptable reliability claims on C&I systems (e.g. considering the expectations expressed in NS-TAST-GD-046 for complex C&I systems);
- it shows an acceptable level of separation of the systems, avoiding interference of lower class systems on higher class systems; and
- it confirms the probabilistic target for the plant can be achieved, as demonstrated by PSA.

95. In relation to the demonstration of diversity claims made in the C&I safety case (i.e. that the primary and secondary protection systems are diverse, and the control systems and the two protection systems are diverse), I judge that Hitachi-GE has considered the main attributes identified in NUREG CR/6303 to ensure sufficient diversity (including technology diversity, human diversity and equipment diversity).

96. With regard to technology diversity, I am content that Hitachi-GE has documented the use of three different technologies for the three main C&I platforms:

- a Class 1 platform based on FPGA, used for the primary protection system (i.e. SSLC);
- a Class 2 platform based on non-complex components (not containing a FPGA or microprocessor), used for the secondary protection system (i.e. HWBS); and
- a Class 3 platform which is microprocessor-based, used for the plant control system and other related C&I systems (e.g. PCntlS and ACS/PCS).

97. I note that the Class 1 and Class 2 platforms are also used for other systems (the SACS and SA C&I respectively), although there is no diversity claim made between these two systems and with any other systems in the C&I architecture.

98. Following my assessment of the platform reports (80, 91, 92 and related documents) and of the Hitachi-GE justification of diversity in a CAE format in Ref. 44, I judge that

the technology used in each platform is sufficiently diverse from the other platforms to be confident that the probability of simultaneous common cause failure of more than one platform is reduced ALARP. A more in-depth assessment of the platforms is provided in section 4.2.3 in this report and in Ref. 34.

99. With regard to human diversity, I judge that, in general, the human diversity requirements in Ref. 40 adequately capture the measures needed to reduce the risk of common cause failures of the C&I platforms, for example by having separate platform design teams within Hitachi-GE with different reporting structures, and using an independent organisation to assess the design, although I note that this was at module level and not board level, and have raised AF-UKABWR-CI-012 relating to this (see Annex 5). Separately, I requested clarification from Hitachi-GE regarding the proposal to use the PCntlS application design team as part of the independent review of the SSLC application design. After clarifications, I note that this approach utilises Hitachi-GE expertise and, at the same time, implements measures to reduce the potential to introduce common cause failures across the independent layers of protection (e.g. requiring a final sentencing of the comments from the internal independent review before implementation of the design).

100. With regard to equipment diversity, I noted during my assessment that it is possible for there to be the same electronic components on different platforms and that this could lead to common cause failure between platforms. These may be complex components (e.g. FPGA's, microprocessors, analogue to digital convertors) or non-complex components (e.g. resistors, capacitors, diodes). In the Topic Report on Hardwired Backup System Platform (Ref. 91) Hitachi-GE presented an analysis of the factors relevant to managing the risk of common cause failures between platforms (specifically the HWBS and Class 1 platform in this case) which identifies a methodology for identifying complex and non-complex common components, and how this will be applied.

101. Hitachi-GE recognise that the manufacturers of C&I systems may subsequently change component supplier, but describe how such changes are identified by Hitachi-GE and decisions taken on potential impacts. For example, Hitachi-GE states that a justification will be provided to show that the impact on the behaviour of affected C&I modules upon failure of the changed components is acceptable, and that a safety justification will review the impact across multiple safety classes. I judge this to be adequate, as this recognises that Hitachi-GE does not have control over other manufacturers' products, and considers the impact on the safety functions being enacted by those components on the affected platform, and more widely.

102. For a platform to be built into a system that can perform safety functions, additional components are required, including sensors, actuators, HMI and systems that support correct operation (such as the supply of electrical power and HVAC). If these contain components that are common with other systems against which diversity is claimed, there is the potential for a common cause to prevent the correct operation of more than one system. However, the selection of sensors, actuators, and HMI and support system components is outside the scope of GDA.

103. I consider that the information provided at this stage of the design in relation to technology, human and equipment diversity (see previous paragraph in this report) is adequate within GDA. Because of the level of maturity of certain C&I systems in GDA (including the selection of the HBWS platform, to be finalised post GDA) and the out of scope items for GDA (e.g. sensors, actuators, and embedded C&I associated with HVAC and electrical systems), I raise an assessment finding for the future licensee to complete the diversity analyses provided in GDA.

*GDA Assessment Finding: **AF-UKABWR-CI-005** - During GDA, Hitachi-GE provided sufficient evidence that principles are in place to ensure adequate*

*diversity between the main C&I systems (e.g. including technology, human and equipment diversity). Post GDA, ONR's expectation is that the detailed design information is used to complete the diversity demonstration.*

*Where claims of diversity are made between C&I systems, the licensee shall complete diversity analyses by using the detailed design information (including sensors, actuators, and supporting systems). This should expand upon the approach applied in GDA, based on NUREG CR/6303, by taking account of other relevant diversity standards and guidance (e.g. IEC 62340 and the regulator consensus document 'Licensing of safety critical software for nuclear reactors').*

*For further guidance see the Technical Observations for AF-UKABWR-CI-005 in Annex 5.*

104. The diversity demonstration shall confirm that the principles established in GDA are correctly deployed in detailed design, e.g. to verify diversity at the component/board level. As appropriate, the demonstration shall analyse the C&I systems for which a diversity claim is made at component level, also considering C&I embedded in supporting systems (e.g. HVAC, electrical supply) and considering sensors and actuators. Whilst addressing this assessment finding, my expectation is that IEC 62340 and the regulator consensus document 'Licensing of safety critical software for nuclear reactors' (Ref. 83) are considered in conjunction with NUREG CR/6303.

105. I also liaised with the ONR PSA inspector with respect to the claims made on the C&I systems in the PSA. I identified that in some instances there is not full consistency between the figures used in the PSA model and the C&I engineering substantiation. For example, in Ref. 62 the reliability data used for the CCF of Class 1 platform components differs from the values justified in the C&I area and a clarification is expected with regards to the reliability modelling in the PSA (e.g. consideration of human actions to avoid an initiating event and exclusion of failure modes, such as SW failures or non-detectable failures, from the causes of an unplanned manual shutdown). I have raised an assessment finding (see AF-UKABWR-CI-006 below) for the licensee to align reliability values between the C&I and PSA disciplines or to justify the reason for the different claims, supporting the C&I technical argument with a PSA sensitivity analysis and a C&I rationale, (e.g. robustness of the system architecture to fault propagation).

*GDA Assessment Finding: **AF-UKABWR-CI-006** - During GDA some differences were identified between the reliability figures used in the PSA and in the C&I substantiation in the safety case. As the PSA model evolves post GDA, ONR's expectation is that the reliability data should align to ensure a realistic estimation of the risk from the plant, unless there is a justification for the difference (e.g. by a PSA sensitivity analysis and a justification as to how the C&I system architecture mitigates the potential for propagation of CCF across the system).*

*The licensee shall ensure consistency between the reliability claims in the PSA and the C&I documentation or substantiate the basis of any difference in the figures.*

*For further guidance see the Technical Observations for AF-UKABWR-CI-006 in Annex 5.*

106. As an overall demonstration that the risk is reduced ALARP for the UK ABWR C&I architecture, I found the argument presented in Ref. 39 sufficiently developed for GDA, because:

- it defines the safety objective to be achieved by the UK ABWR;
- it identifies the gaps to be covered in comparison with the reference design; and
- it provides evidence of optioneering to reach the optimal solution for the UK ABWR.

107. I note that additional C&I systems were discussed in the latter stages of GDA as part of FS discussions (see e.g. the proposal for a Class 1 C&I system, the Axial Peaking Power Range Monitor (A-PPRM), for the all rod insertion scenario in Ref. 82). My expectation is that, as the UK ABWR C&I safety case is developed post GDA, any proposed C&I systems are properly justified in the context of the overall C&I safety case, including but not limited to providing an adequate demonstration of its reliability, segregation, independence and diversity as necessary.

108. In conclusion, I found that the overall C&I architecture proposed for the UK ABWR is adequately substantiated for GDA.

### 4.2.3 C&I Platforms

109. Hitachi-GE submissions (e.g. Ref. 44) state the UK ABWR has three main C&I platforms:

- Class 1 vCOSS®/NCFS-1
- Class 2 Hardwired Platform
- Class 3 HIACS

110. I assessed the suitability of each of the main UK ABWR C&I platforms to support the reliability and other requirements placed on them by the safety analyses, considering relevant standards and guidance, and other requirements such as diversity.

111. The outcome of my assessment is presented in this section of my report.

#### 4.2.3.1 The Class 1 platform

112. The Class 1 platform was developed during the UK ABWR GDA project. The design was started early in GDA, and whilst it has not been completed by the end of Step 4, good progress has been made, and the documentation produced is sufficient for me to perform an assessment.

113. The SSLC is based on the vCOSS®/NCFS-1 platform which uses Field Programmable Gate Array (FPGA) technology. This technology is diverse from the other two main C&I systems (see section 4.2.2 on architecture).

114. The Class 1 platform has to support the functions required by the systems that use this platform, namely the SSLC and the SACS, with the required reliability.

115. During my initial assessment of the Class 1 platform submissions I was not able to identify where the relevant lifecycle activities referenced in IEC 61513 and described in IEC 61508 had been documented. I raised RQ-ABWR-1035 (Ref. 37), requesting information on where the lifecycle activities were documented, seeking assurance that the content of these achieves the intent of the relevant standards, requesting information on the source of the Safety Requirements Specification (SRS), and how functional safety assessment (FSA) will be carried out.

116. The Hitachi-GE response to RQ-ABWR-1035 (Ref. 111) identified the documents in which the lifecycle activities are documented, confirming that the contents of the documents are based on the relevant clauses of IEC 61508, notifying ONR of a documentation change to clarify the source of the SRS, and outlining the functional safety assessment (FSA) activities through improvements to documentation.

117. I am satisfied with this response and have subsequently confirmed that the lifecycle activities have been adequately documented, the source of the SRS is adequately clear, and that FSA activities have been clarified, as detailed in my assessment below.

**Class 1 platform Categorisation and Classification**

118. Safety analyses performed by Hitachi-GE and documentation (see section 4.2.2 on architecture) state that the SSLC platform has to perform Category A safety functions and is Class 1 with a reliability requirement of $10^{-4}$ pfd.

119. Hitachi-GE provided a number of submissions that describe the design process for the Class 1 platform hardware, including the Topic report on the Class 1 Platform (Ref. 80) which references IEC 60780 for equipment qualification.

120. The Safety Plan for NCFS-1 (Ref. 56) provides more detail on the hardware design and development process, referencing the relevant parts of IEC 60987 (for hardware design), IEC 62566 (for FPGA design relating to Category A functions), IEC 61513 (relating to safety design lifecycle) and IEC 61508 (relating to hardware design techniques and measures). I note that IEC 60987 relates to the hardware design requirements for computer based systems, but I consider this to be applicable for the FPGA based Class 1 platform as the requirements are similar, meeting my expectations in relation to ECS.4.

121. I assessed the approach to the design and development of the hardware of this FPGA based platform, referencing this against these standards and guidance. For example the Safety Plan for NCFS-1 (Ref. 56) provides a clause by clause description of how the requirements of each standard have been satisfied (i.e. Appendix C covering IEC 61513, and Appendix D covering IEC 60987, IEC 61508 and IEC 62566), and where the evidence of this may be found. The references for the location of the evidence are specific, and my sampling of this has confirmed that the evidence is sufficient to confirm the intent of the relevant parts of the standards has been addressed (e.g. the lifecycle activities, contents of the SRS and FSA in IEC 61508).

122. I am satisfied that the general approach to the hardware design and development of the Class 1 platform meets my expectations, as described by ECS.3, and judge the approach to be adequate for the purposes of GDA.

123. However, I noted that details of the calculations to determine safe failure fraction and diagnostic coverage have not been provided during GDA. These are important, as they underpin the adequacy of the SSLC modules in supporting the systematic integrity of the SSLC systems. The importance of these is such that I judge it appropriate to raise an assessment finding on this topic.

> *GDA Assessment Finding: **AF-UKABWR-CI-009** - During GDA Hitachi-GE provided an adequate demonstration that SSLC hardware reliability would achieve its targets. Post GDA ONR's expectation is that as the detailed design is developed, a full justification of key parameters (such as safe failure fraction and diagnostic coverage) is provided, taking into account, for example, the guidelines in Annex C of IEC 61508-2:2010 for SSLC modules*
>
> *The Licensee shall substantiate safe failure fraction and diagnostic coverage claims for all SSLC modules, and confirm the C&I system meets reliability targets, taking into account the overall system architecture.*

### Class 1 platform production excellence process

124. The submission “Detail Project-Schedule for New Class 1 Platform” (Ref. 85) describes the activities to be carried out to develop the Class 1 platform production excellence (PE) activities and the documents to be delivered during GDA. I judge this to be adequately detailed and to correctly identify which activities should be undertaken, and when those should be undertaken.

125. The Safety Concept (Ref.86) describes how the Class 1 platform will be configured into a system that can perform the safety functions required of the SSLC and SACS. This provides context in respect of the platform module designs presented during GDA, and how the overall system will be qualified.

126. The Safety Plan (Ref. 56) describes the design and development process for the SSLC platform. This is in the form of the definition of the safety lifecycle and the techniques and measures applied to ensure the SSLC platform meets its design intent.

127. I have sampled the safety lifecycle, and the techniques and measures that have been applied to ensure the SSLC platform meets its design intent, whether the requirements of relevant standards and guidance have been met, and whether the overall claims have been met by the design process and output documentation.

128. Hitachi-GE claims relevant modern standards have been applied to the SSLC design, for example the Basis of Safety Case on the Class 1 platform lists applicable standards, including IEC 61513, IEC 60987, IEC 62566, IEC 60880, and IEC 61508.

129. The Safety Plan (Ref. 56) describes in detail how the clauses have been addressed for IEC 61513 (in Appendix C), IEC 60987 (in Appendix D), IEC 62566 (in Appendix A), IEC 60880 (in Appendix A), and IEC 61508 within the body of the report.

130. I have sampled the evidence relating to standards and have confirmed that suitable standards have been referenced, and that appropriate clauses of these standards have been addressed through the process submissions. The majority of standard clauses have been met, but where a shortfall has been identified an explanation is given, and additional measures identified or a justification provided. Evidence documents are identified with specific reference to the section in which the evidence is given.

131. I note that IEC 60880 applies to the development of software performing category A safety functions, but the Class 1 FPGA platform does not use conventional software. Hitachi-GE has recognised the importance of this standard, performed a clause by clause analysis that treats the FPGA configuration process as software, and demonstrated that the platform development process complies with these. I consider this to be good practice.

132. I have also assessed the adequacy of the design process against relevant guidance and UK RGP, including NS-TAST-GD-046 (Ref. 7), and am satisfied that Hitachi-GE design process is adequate for the Class 1 platform, covering both hardware and FPGA configuration, that this is reflected in the design documentation, and that Hitachi-GE has demonstrated that this meets the intent of the relevant standards and guidance, with the one exception described below.

133. I did identify a potential shortfall in the area of verification of the FPGA design. Hitachi-GE describe who will be responsible for verification in the various lifecycle phases in Table 1.4.4-1 of the Safety Plan, (Ref. 56). Some of the board level verification activities are performed by the team leader. Because the team leader is not independent from the design, there is the potential for a misinterpretation of

requirements to occur and for the same misinterpretation to occur in the verification. Clause 9.1.1 of IEC 62566 states that the verification team shall be composed of individuals who are not engaged in the development, and then further describes independence requirements. I note that this requirement is similar to section 8.1 of IEC 60880 that relates to the development of software for Category A safety functions.

134. I raised this with Hitachi-GE, who documented an analysis of independence of verification in the Safety Plan (section 1.3.5.3 in Ref. 56). This indicates that where the designer misinterprets the SRS and Safety Concept, independent verification is achieved by simulation and test activities. Whilst these are valuable activities, in my opinion, they do not challenge the correctness of the design in the same way as an independent verification of the design components. I therefore raise an assessment finding.

> *GDA Assessment Finding: **AF-UKABWR-CI-012** - During GDA Hitachi-GE identified an adequate approach for the overall independent verification of the safety class 1 platform at module level but did not adequately address independence of verification at lower levels (e.g. at printed circuit board level). Post GDA the safety case should clarify the arrangements proposed for the verification of the safety class 1 platform at all appropriate levels.*
>
> *The licensee shall review compliance against relevant standards (e.g. IEC 62566, IEC 60880) to ensure independent verification is performed on the safety class 1 platform at all appropriate levels, providing adequate justification that measures to detect errors will be effective in reducing risks so far as is reasonably practicable.*
>
> *For further guidance see the Technical Observations for AF-UKABWR-CI-012 in Annex 5.*

135. The platform development process is dependent upon the use of computer based tools for conversion of the design from one format to another, equivalence checking, and reporting of anomalies. I was concerned that a fault in one or more tool has the potential to introduce an error in the design which could lead to a safety impact. I therefore sought assurance that Hitachi-GE has considered the consequence of tool faults, how these could be identified, and what actions would be needed to prevent a fault being introduced into the platform design.

136. Hitachi-GE submitted an evaluation of design tools (Ref. 87) describing in detail the tools used in the platform development, and documenting the results of a Hazard and Operability study (HAZOP) performed on each of these, covering the potential consequence of a tool fault when used as described in the development process, and identifying mitigation measures.

137. My assessment determined that the HAZOP process appears to be suitable to detect the consequence of tool faults and to have been appropriately applied (e.g. guidewords specific to the task were identified, with appropriate attendance from the platform designers). It is my opinion that the hazard based approach taken will be effective at managing risk when a tool version changes (although I also note that Hitachi-GE has a policy in place to avoid the use of new versions of tools where possible). However, the document does not state how actions identified from the HAZOP will be applied to the platform development process (see point (a) of AF-UKABWR-CI-013 below).

138. My assessment of the document “Formal Verification Result” (Ref. 135) found that “deadcodes” have been identified by the formal verification. Dead code is a term applied to software that will never be executed because it cannot be reached by the

microprocessor under normal operational conditions. In relation to the FPGA configuration for the SSLC platform, dead code relates to logic that is specified but which cannot perform a function because it is not connected in such a way that it will affect system output. However, the documentation does not provide any further information regarding the nature or connectivity of the unused logic or make a case that this logic cannot influence the operation of the platform under all circumstances. For this reason I raise point (b) of Assessment finding AF-UKABWR-CI-013.

> *GDA Assessment Finding: **AF-UKABWR-CI-013** - In GDA, Hitachi-GE identified a set of software tools to be used in detailed design for the development of the safety class 1 platform and application, and analysed the consequences of their failures and limitations. As the design is further developed, evidence will need to be produced on the effectiveness of the overall set of tools to detect and mitigate faults.*
>
> *The licensee shall clarify:*
>
> *a. How the measures identified to detect and mitigate tool faults have been applied; and*
>
> *b. The consequences of logic with no apparent function on simulation coverage, and the significance of this on the safety demonstration.*
>
> *For further guidance see the Technical Observations for AF-UKABWR-CI-013 in Annex 5.*

139. The Safety Plan (Ref. 56) states that macros will be used in the Class 1 platform. Macros are pre-developed complex functions that could be replicated multiple times within a design, and a fault in a macro has the potential to introduce that fault into areas of the design with unpredictable consequences. Some macros are to be developed and verified by other parts of Hitachi not associated with the platform design.

140. Whilst some of these macros can be fully formally verified, others have too large a verification space for this to be practical. Hitachi-GE describes the partial verification of macros by combining static and dynamic techniques to provide confidence these do not contain faults. Dynamic verification is described, with the verification space reduced by several techniques and measures, so that the verification can be completed within a realistic timeframe." I consider this is adequate for GDA, but have a residual concern that a macro could exhibit unexpected behaviour due to undeclared functionality, and that an undetected fault could be introduced into the platform implementation and any applications that need to use this macro. I therefore raise an assessment finding for improved justification to be made in this area post-GDA.

> *GDA Assessment Finding: **AF-UKABWR-CI-010** - In GDA, Hitachi-GE identified a number of measures to verify the library functions/macros to be used in the safety class 1 platform. ONR's expectation is that during the detailed design an adequate justification is provided that demonstrates that risks arising from the use of library functions/macros have been reduced ALARP.*
>
> *The licensee shall provide justification that pre-developed library functions/macros used in the FPGA design have been adequately verified, do not interfere with other functions, do not have unintended side effects, and do not contain unexpected functionality.*

### Class 1 platform independent confidence building measures

141. In submissions (e.g. Refs. 80, 88), Hitachi-GE identified the need to perform independent confidence building measures (ICBM's) on the Class 1 platform to meet regulatory expectations such as those described in NS-TAST-GD-046 (Ref. 7). Also that ICBM measures should be diverse to those applied during PE activities.

142. Recognising that the platform design would not be completed by the end of GDA, but that it would be necessary to demonstrate that ICBM's could be practically applied to the Class 1 platform, Hitachi-GE assessed the feasibility of performing ICBM's on the Class 1 platform, using a specialist UK contractor.

143. The Topic Report on ICBM for FPGA (Ref. 88) describes a number of potential ICBM's identified that could be diverse from PE measures, including:

- Statistical Testing (ST)
- Concurrency analysis
- Worst Case execution time analysis
- Equivalence checking
- FPGA configuration verification (Bitstream verification)

144. In respect of ST, Hitachi-GE identify a number of features that are necessary to ensure its practicality and feasibility, including the ability to reset the system to a known state within a short time and that an Oracle can be built from the documentation available. Hitachi-GE has confirmed that ST of a system built on the Class 1 platform is feasible because the system can be reset by removing power, and that powering up takes a short time before the system is available for the next test. In this way the feasibility of performing a large number of statistical tests (i.e. in the order of 50,000 tests in accordance with Ref. 7) has been demonstrated. Hitachi-GE has also confirmed that the documentation is suitable for an Oracle to be built. The information presented during GDA is adequate and my expectation is that post-GDA, and at an appropriate time, the licensee will undertake sufficient statistical testing to underpin the safety case for the SSLC, considering functional differences between divisions.

145. I wished to confirm that ST would be feasible and valid, and raised RQ-ABWR-0624 requesting further information on ST documentation suitable for transfer to a future licensee and on the validity of ST. In the response, Hitachi-GE listed the information needed for ST to be carried out. I am satisfied that this will be suitable for the future licensee to carry out ST post-GDA.

146. Hitachi-GE confirmed the feasibility of concurrency analysis, covering the overall FPGA-based platform architecture. I concur with the finding and judge this to be adequate.

147. Review of the feasibility of worst case execution time analysis concluded that this is possible, but is best achieved using dynamic analysis. I judge that this will be effective in identifying system configuration related timing limitations.

148. Hitachi-GE concluded that equivalence checking is not a valid ICBM because this is done as a part of PE (as a compensating measure). Therefore this is not proposed as an ICBM and I concur with this.

149. The FPGA design is encrypted before being sent to the FPGA chip using a process called Bitstream. The encryption is proprietary to the FPGA manufacturer, so it is not possible for Hitachi-GE to confirm the design has been correctly inserted into the FPGA. Neither is it possible to read back the FPGA contents to confirm its correct configuration. This is a well understood limitation of the use of FPGA's, is referenced in relevant standards (e.g. IEC 62566), and is acknowledged by Hitachi-GE.

150. I observe that FPGA's have been successfully used in high integrity safety applications in a number of industries, and that techniques such as statistical and dynamic testing increase confidence the FPGA is correctly configured, and are likely to improve control of risks arising from FPGA misconfiguration. However, additional measures to further reduce risks may be reasonably practicable, and I judge that the future licensee should identify and investigate potential additional measures and the feasibility of these post-GDA. I therefore raise this as an assessment finding.

> *GDA Assessment Finding: **AF-UKABWR-CI-008** - Hitachi-GE has identified a variety of techniques and measures for the verification of the various steps in the FPGA development during GDA. ONR's expectation post GDA is that further work is carried out to identify if there are any additional measures that can be applied to the verification of the FPGA configuration (for example, using the outcome of CINIF research).*
>
> *The Licensee shall undertake an options analysis exercise to determine what additional measures could be applied to confirm the correct internal configuration of the safety class 1 platform FPGA, report on the findings, and determine, so far as is reasonably practicable, if any of the identified measures should be applied.*

151. Regulatory observation RO-ABWR-0029 (Ref. 17) (see Annex 4) related to the development of the Class 1 platform. I raised a number of RQ's relating to this during GDA Step 4 and Hitachi-GE responded adequately to these, clarifying the details of the development process, and improving documentation to provide a more complete justification. I concluded that these improvements were sufficient for RO-ABWR-0029 to be closed.

152. Regulatory observation RO-ABWR-0032 (see Annex 4) was raised during GDA Step 3 and related to the design of the Class 1 platform, covering the design and development lifecycle, the schedule of the development, the use of independent organisations, and confirmation that the design and development will reach a suitable level of maturity during GDA to enable a meaningful assessment to be carried out. Hitachi-GE delivered further submissions during GDA Step 4 and I raised a number of RQ's relating to these on test coverage, design and verification, lifecycle and equipment qualification. The Hitachi-GE responses were adequate, with significant improvements to the documentation that provided a demonstration of adequacy. I concluded that these improvements were sufficient for RO-ABWR-0032 to be closed.

**Configuration of the Class 1 platform**

153. Depending on specific application requirements, the Class 1 platform will contain parameters that need to be modified during the life of the plant (e.g. neutron flux detector calibration).

154. During GDA Step 4 Hitachi-GE provided documentation to describe how the Class 1 platform configuration is stored, and how these configurations may be modified (Ref. 86).

155. My assessment of the adequacy of the parameter setting mechanism of the Class 1 platform questioned whether there is adequate protection against hazards that could cause misconfiguration of the Class 1 platform and hence subsequent misoperation of the SSLC, including the potential for the SSLC to be unable to respond to safety demands.

156. I determined that the hazards that could cause misconfiguration of parameters include:

- re-configuration at the wrong time (e.g. whilst the SSLC is operating);
- inadvertent configuration with the wrong values;
- inadvertent configuration of the wrong parameters; and
- failed configuration.

157. The sources of these hazards include human errors, a fault with the equipment used to modify parameters, and a fault in the Class 1 platform components.

158. The Safety Concept (Ref. 86) states that the Class 1 platform parameters are modified only according to a predefined procedure using a dedicated tool. The tool is not connected during normal operation.

159. To prevent parameter modification at the wrong time, there are a number of measures including a mechanism built into the Class 1 platform hardware to prevent the parameters being changed whilst the Class 1 platform is online. This is engineered using the same design processes as the Class 1 platform. I judge that the measures will be effective against each of the hazard sources described above to prevent parameter modification at the wrong time.

160. The communications are designed so that access to the parameters is only possible during specific system conditions in combination with the use of a dedicated tool. For this reason I judge that the design adequately prevents parameters in other racks being inadvertently modified.

161. I note it is still possible for human error, a fault with the equipment used to modify parameters, or a fault with the Class 1 platform to cause parameters to be incorrectly set. The Safety Concept (Ref. 86) document and other documentation (e.g. the Conceptual Security Analysis, Ref. 78) describe how the plausibility of the parameters is checked. However, further information will be required post-GDA justifying that adequate measures are put in place to ensure that the Class 1 system remains correctly configured. I have raised this as AF-UKABWR-CI-019 below.

> *GDA Assessment Finding: **AF-UKABWR-CI-019** - In GDA, Hitachi-GE described a number of different measures to ensure that the terminal used to configure the SSLC, cannot interfere with its correct operation or introduce faults in the system. ONR's expectation as the design develops post-GDA is that evidence is provided the selected measures are shown to reduce the risk ALARP.*
>
> *The licensee shall provide an ALARP demonstration to show that the risk of faults introduced by the terminal used to configure the SSLC is adequately controlled, including a demonstration that:*
>
> *a. Connection of the terminal will not interfere with the ability of the SSLC to respond to demands.*
>
> *b. The terminal cannot modify parameters that are not intended to be changed or it can be confirmed with sufficient integrity that other parameters have not been changed.*
>
> *c. There is an adequate means of confirming correct parameter entry, storage and use within the SSLC.*

162. Other parts of the Class 1 platform also need to be correctly configured (e.g. the calibration of Analogue Input (AI) modules). Similar measures to prevent unauthorised configuration change are implemented.

163. My assessment has considered a range of hazards that may prevent the correct operation of the Class 1 platform due to incorrectly set parameters, and examined the measures used to prevent or mitigate the effect of these. I judge that the measures described will be adequate to prevent incorrect or inadvertent modification of parameters.

164. In conclusion, I judge that the information relating to design and development of the Class 1 platform, including PE and ICBM's, use of tools, and configuration are adequate for GDA, noting that I have raised a number of assessment findings in this area.

#### 4.2.3.2 The Class 2 platform

165. The hardwired backup system is a secondary means of bringing the plant to a safe shutdown state under fault conditions for frequent faults and in the event of a common cause failure affecting both the plant control system, and the primary safety systems.

166. During GDA Step 4 Hitachi-GE informed ONR that the Class 2 platform for the HWBS would not be selected during GDA for project and commercial reasons. I accepted this on the basis that during GDA Hitachi-GE would determine the requirements for the HWBS and its platform, and provide sufficiently detailed information on one platform to demonstrate it is feasible for a hardwired platform to achieve the necessary functional and reliability requirements. This change in approach affected RO-ABWR-0027 action 2 (Ref. 15), with ONR agreeing to change the wording of this action, see Annex 4.

167. I raised RQ-ABWR-1430, asking for information on how Hitachi-GE would, during GDA, clarify the technical basis for selecting the technology for the hardwired backup system platform. i.e.:

- identify what criteria should be considered in selecting the HWBS platform;
- determine the adequacy of the design development process;
- determine the testing and qualification regime; and
- determine the operational and maintenance requirements.

168. Hitachi-GE responded (Ref. 89), stating that two potential HWBS platforms have been identified as suitable, and that one of the potential platforms will be described in GDA, to demonstrate feasibility. Also that this potential platform and it's attributes would be described in the Basis of Safety Cases on HWBS (Ref. 47), Topic report on the HWBS (Ref. 90), and Topic report on the HWBS platform (Ref. 91). I accepted this response, and assessed the submitted documents.

169. The Hitachi-GE submission "Basis of Safety Cases on Hardwired Backup System" (Ref. 47) provides an overview of the requirements of the hardwired backup system, noting that this must be a system that avoids the use of the fundamental technologies that are used in the other two main C&I systems, namely microprocessors and complex configurable devices. Also that equipment supporting the operation of the HWBS, such as the electrical power system and HVAC and other equipment necessary for its operation such as sensors, HMI, and actuators, will not use these technologies. Further information on my assessment of the in-scope aspects of this are given in the systems and diversity sections of this report (sections 4.2.4 and 4.2.2, respectively).

170. The Basis of Safety Cases on Hardwired backup system (Ref. 47) states that the hardwired backup system platform will be purchased from a supplier external to Hitachi-GE to reduce the potential for common cause failure. The diversity requirement is adequately captured in the claims and arguments, although I note that diversity analysis will be required to confirm this post-GDA (see AF-UKABWR-CI-005). This document also describes the requirements of the HWBS using a CAE approach to

determine the classification of the HWBS, which standards the system (and platform) should comply with, and functional and non-functional requirements. This determines the HWBS should be capable of performing Category A safety functions as a second layer of protection (hence Class 2) and a reliability of $10^{-2}$ pfd. I have assessed the suitability of the HWBS platform on this basis and judge the CAE to be sufficiently developed to allow a meaningful assessment to be carried out.

171. The Topic Report on Hardwired Backup System Platform (Ref. 91) provides a description of a potential HWBS platform, and the non-functional requirements as SPCs. I note that functional requirements are specified in other documents such as the Topic report on the Hardwired backup system (Ref. 90), and various other documents such as interlock block diagrams (IBD's) and instrument lists (INL's).

172. This document (Ref. 91) describes the basic specification of the HWBS platform and the platform design features required to fulfil the SPCs, also providing a number of data sheets for a potential platform, including diversity and reliability calculations.

173. My assessment of the basic specifications for the HWBS revealed that the key criteria are adequately defined (e.g. the diversity, reliability, independence, testability, and single failure criterion requirements) and that the system level specification is similarly defined (e.g. the input, divisional, output, voting arrangements, and normal actuation and failure output states). This meets my expectations as the features of the hardwired backup system platform required to fulfil the hardwired backup system requirements have been adequately defined for GDA.

174. I sampled aspects of these requirements in relation to the suitability of the prospective HWBS platform.

175. In respect of diversity, I note that some evidence is provided in the form of representative component by component analysis against the Class 1 platform covering resistors, inductors, diodes and transistors, with reference to relevant standards (e.g. NUREG CR/6303). The outcome of this preliminary analysis indicates that there is diversity of manufacturer for each of these component types, but also establishes the principle of diversity analysis at a component level. I am satisfied this is suitable for GDA.

176. In respect of reliability, I note that the evidence provided indicates that the prospective HWBS platform is capable of achieving the target reliability and that the analysis is adequately detailed for the purposes of GDA. For example, sample module reliability and system reliability calculations have been provided, taking into account system architecture and diversity limitations. I have not assessed these calculations in detail, but note that these indicate that system reliability requirements can be met by the prospective platform by some margin. I also note that relevant standards have been referenced in respect of these calculations (e.g. IEC 61508 part 6, Annex D), FMEA's are provided, and these give adequate confidence for the purposes of GDA that the reliability calculations post-GDA can be adequately substantiated. My expectation is, when the HWBS platform is selected and the system design completed, that the licensee will confirm and substantiate the reliability of the HWBS using methodologies equivalent to those presented in GDA.

177. In respect of independence, the Topic report on Hardwired Backup System Platform (Ref. 91) gives a description of the features of the potential HWBS platform that will ensure independence between the HWBS divisions and other system platforms. In particular, I judge the principle of electrical independence is adequately established and the measures proposed are suitable (e.g. use of relays of appropriate voltage isolation capability and galvanic isolation devices).

178. In respect of testability, Hitachi-GE note that the proof test interval for the HWBS is 18 months and this means that no online proof testing is necessary. The principles of offline proof testing are briefly described, considering the modularised functionality of the HWBS and the capability of the prospective platform components. Hitachi-GE states that a proof test strategy will be developed post-GDA, based upon the capability of the selected platform and safety manual, and an example arrangement is outlined. This gives me confidence that offline proof testing of the HWBS platform is feasible and that an adequate testing strategy can be established post-GDA when the platform has been selected. However, it is important that the reliability of the HWBS will be adequately justified post-GDA, and this is the subject of point (c) of AF-UKABWR-CI-014 below.

179. In addition to the HWBS design attributes described above, Hitachi-GE has outlined a design process by which the platform components will be integrated into a system that achieves the required properties. This follows the lifecycle approach outlined in IEC 61513 and IEC 61508, covering the platform development process (noting that the outline platform design has been completed and has previously been assessed as compliant and suitable for high integrity applications), suitability analysis, system design, detailed design, implementation, testing, installation, operation, maintenance, and modification. This outline process meets my expectations as it references relevant standards and if followed, is likely to meet regulatory expectations during post-GDA design activities.

180. I have also assessed the integration of the platform documents into the safety case, and the adequacy of referencing. I found that there is adequate description of how SFCs will be satisfied by the system and how this relates to the platform attributes. I also found that SPCs associated with the platform have been adequately referenced for the purposes of GDA, with SPC arguments satisfied by each relevant section in the topic report being listed. I note that more detail will be required during detailed design, but judge this to be adequate for the purposes of GDA.

181. During my assessment I noted that accurate measurement of reactor coolant level using differential pressure requires correction due to density changes arising from variations in temperature. Correction for this may be important for safety, and the HWBS platform may need to perform this correction. The safety case does not appear to have identified this as a safety requirement, but if necessary, it is an important requirement for the HWBS platform selection. For this reason I raise this as point (a) of assessment finding AF-UKABWR-CI-014 below.

182. Similarly I have identified a functional requirement from my assessment on testing and maintenance (see section 4.2.7) that identifies a need to temporarily change the voting configuration to facilitate testing (for example where an in-service failure is identified, a component is replaced, and testing of the restoration of correct operation is necessary). It is not clear to me that the implications of this functional requirement have been clearly identified such as the potential for the voting arrangement to be left in the wrong configuration, and for this reason I raise this as point (b) in assessment finding AF-UKABWR-CI-014.

> *GDA Assessment Finding: **AF-UKABWR-CI-014** - During GDA Hitachi-GE provided an adequate demonstration of the suitability of the HWBS architecture and diversity requirements and have identified candidate platforms that can deliver these. ONR's assessment identified that not all system requirements may have been identified during GDA, and expects that the suitability of the site specific HWBS is substantiated when all requirements have been identified during detailed design.*
>
> *The licensee shall:*

a. *Ensure that the use of set points for RPV water level trips is compatible with the licensee's concept of operation and is derived from the site specific fault studies, and identifies the potential need for the HWBS platform to have the capability to correct for water density changes (over all relevant temperature conditions).*

b. *Justify the suitability of the configuration of the voting arrangements, considering testing and maintenance requirements, and how the risks arising from this will be adequately managed.*

c. *Confirm and substantiate that adequate HWBS reliability can be maintained under all operational conditions, considering the number of divisions and the requirement to test and maintain equipment (including plant equipment).*

d. *Confirm the selected HWBS HMI technology meets relevant safety case requirements, particularly in relation to the use of non-programmable components.*

*For further guidance see the Technical Observations for AF-UKABWR-CI-014 in Annex 5.*

183. In conclusion, my assessment of the Class 2 platform documentation found this to be adequately developed, appropriate standards have been referenced, a suitable design lifecycle has been described, and sufficient detail has been provided to give confidence that a suitable HWBS platform is available to support the UK ABWR C&I design architecture.

184. ONR raised RO-ABWR-0027 during GDA Step 2 because Hitachi-GE had not provided sufficient information on the Hardwired Backup System (HWBS) for an assessment to be carried out. During GDA step 4 Hitachi-GE provided a comprehensive list of safety function requirements for the HWBS linked to the UK ABWR main reactor fault schedule (Ref. 42) and the fuel route (Ref. 43), and documentation to justify the design, design process, prospective HWBS technology, and system architecture. This meets my expectations for the purposes of GDA, and I closed RO-ABWR-0027.

185. In summary, I conclude that Hitachi-GE has provided suitable documentation that describes the design and development process and potential technologies that may be used for HWBS and how the design may mitigate against common cause and systematic failures between platforms with different classifications. I consider the proposed platform is adequate to demonstrate during GDA that the HWBS technology is feasible, and that the identified methodology to test the diversity of the HWBS platform is adequate.

#### 4.2.3.3 The Class 3 platform

186. The Class 3 platform is the basis for the PCntIS and is directly classified, according to IAEA SSG-30, as Class 3.

187. The document Topic Report on Class 3 platform (Ref. 92) states the Class 3 platform is based on HIACS, a general purpose microprocessor-based industrial systems controller running the Compact Process Monitoring System (CPMS) operating system. HIACS based systems consist of at least one controller, I/O modules, and a communication system housed in a rack containing a power supply and other equipment. HIACS is capable of single controller, duplex, and triplex operation.

188. HIACS applications are programmed using software called PADT (Programming and Debugging Tool) that allows the user to visualise the logic as a hierarchical Software Logic Diagram (SLD). This runs on a PC and the PADT output is loaded into the HIACS controller using Ethernet communications.

189. In accordance with the Step 4 GDA C&I sampling strategy, my assessment of HIACS was limited to determination of the feasibility of HIACS to support the functions required of the plant control system, consideration of relevant standards and integration of the safety Claims Arguments and Evidence with the Class 3 platform.

190. My assessment of the feasibility of HIACS to perform the necessary functions is informed by the Topic Report on Class 3 platforms (Ref. 92) with section 4 of this document describing the UK ABWR Class 3 functional systems and their connectivity. This also describes the level of redundancy required for each (e.g. Triplex for the APR, FDWC, RFC, and Duplex for the RCIS and reactor/turbine auxiliary system).

191. The Topic Report on Class 3 platforms also shows the data connection interface from the Class 1 platform to the Class 3 data bus using appropriate one way communication and isolation devices (qualified at Class 1). This confirms the ability of the Class 3 platform to receive information from the Class 1 SSLC without influencing the higher class system. Sufficient information is provided for the purposes of GDA of how the duplex and triplex configurations react to failure. In particular I note the presence of hardware relays to physically disconnect failed controllers in the Triplex configuration. The document provides outline hardware reliability calculations for platform modules and whilst I have not confirmed the correctness of these, conservatisms are described that give me confidence the target reliability will be met by a system built on this platform.

192. I note that a diversity analysis has been performed on the Class 3 platform using NUREG CR/6303 that considers its diversity with the other main C&I platforms, covering human diversity, design diversity, equipment diversity, and software diversity. This demonstrates that the Class 3 platform has adequate diversity from the other main C&I systems.

193. My assessment of the standards applied to the Class 3 platform identified that relevant standards (including IEC 61513, 62138, 61508, and the 61000 suite of standards for EMC) are referenced as applicable to the HIACS platform. Analysis of compliance of HIACS with these was not provided during GDA but section 5 of Ref. 92 states that compliance with these will evaluated during the site specific phase. For the purposes of GDA I do not have any specific concerns in this area, as the HIACS lifecycle process is outlined in the document, and this appears similar to that referenced in the relevant standards. However, a positive outcome from this evaluation and suitable measures will be necessary to underpin my assessment and confirm the suitability of the Class 3 HIACS platform and the application of this in the PCntlS.

194. My assessment of the Topic report on the Class 3 platform (Ref. 92) found multiple links to the wider PCntlS SPCs, providing evidence that these SPCs have been met by the platform. Whilst further development is required, I am of the opinion that the Class 3 HIACS platform has adequate safety links for the purposes of GDA.

195. During my assessment I identified one concern regarding the demonstration of the adequacy of the Class 3 platform to meet timing requirements. The Class 3 platform TR states that “The adequacy of the response time for UK ABWR will be demonstrated by plant performance test and/or plant start-up test”. This does not meet my expectations as it is difficult to determine worst case response times of distributed C&I systems by testing alone. My expectation is that analysis of expected response times, confirmed by testing would provide a significantly better understanding of system

performance and confidence that required performance will be achieved under all relevant conditions. I therefore raise this as an assessment finding.

> *GDA Assessment Finding: **AF-UKABWR-CI-015** - During GDA, Hitachi-GE provided a justification of the PCntlS meeting its performance requirement based on testing. ONR's expectation is that, once the detailed design architecture of the system is finalised, additional confirmation of the PCntlS response time will be provided.*
>
> *The licensee shall confirm the performance of the PCntlS using an appropriate combination of analysis and testing to provide confidence that the PCntlS can achieve performance requirements under all relevant conditions.*
>
> *For further guidance see the Technical Observations for AF-UKABWR-CI-015 in Annex 5.*

196. In conclusion, my assessment considered the feasibility of the Class 3 platform to perform the functional requirements placed on it, compliance with relevant standards, and integration into the UK ABWR C&I safety case, has found that the Class 3 HIACS platform to be suitable, subject to further work to be completed during the site specific phase of the project.

#### 4.2.3.4 Conclusion of platform assessment

197. My assessment of the Class 1 platform development, proposed Class 2 platform, and aspects of the Class 3 platform gives confidence that each platform is capable of meeting the fundamental functional and non-functional requirements expected for the UK ABWR C&I systems and of meeting UK regulatory expectations subject to addressing the assessment findings during subsequent licensing and construction activities by a future licensee. My expectation is that future activity during detailed design will be necessary to confirm that this is the case, considering the site specific inputs to SFCs/SPCs, diversity and reliability.

### 4.2.4 C&I Systems

198. This section describes the outcome of my assessment of UK ABWR C&I systems and builds upon the assessment of safety case, architecture and platforms. Progress with resolution of regulatory observations raised during earlier GDA steps and relating to systems is identified and reported.

199. The focus of my assessment of systems has been the evidence of the adequacy of the main properties of the systems (e.g. resistance to single failure, adequate redundancy, etc.).

#### 4.2.4.1 Safety System Logic and Control

200. The PCSR chapter 14 (Ref. 39) states that the SSLC is the primary protection system for the UK ABWR, based upon the Class 1 platform, and has four divisions of C&I equipment configured in a 2 out of 4 (2oo4) voting arrangement to initiate a reactor trip, isolate the primary containment, and actuate the three divisions of mechanical plant for core cooling.

201. Hitachi-GE documentation states each division of the SSLC is separated from the others electrically and physically, and is divided into two sub-systems:

- the RPS / MSIV which inserts control rods and closes the main steam isolation valves; and

- the ECCS / ESF which maintains core coverage, provides decay heat removal and related functions including containment isolation.

202. Further information on the arrangements to ensure the SSLC is separated and isolated from other C&I systems, and that the divisions are adequately separated is given in the Topic Report on Safety System Logic and Control System (Ref. 104), with reference to the SPCs for which the evidence is being given. I note that this document references IEC 60709 for evidence and provides detail of physical separation of C&I panels and cabling. This meets my expectations for the purposes of GDA in that the C&I panels and cabling are shown separated, and that optical fibres are effective in providing electrical isolation between divisions. I judge this to be adequate, but note that the final layout and cabling arrangements will not be confirmed until detailed design has been completed. It is my expectation that the future licensee will demonstrate that the SPCs and relevant standards have been met by the design so far as is reasonably practicable, and the effectiveness of separation to protect against relevant design basis hazards.

203. The PCSR chapter 14 describes the inputs to the SSLC necessary to perform the RPS and MSIV functions. I have not assessed these in detail during my assessment as these have been considered in other ONR assessments. However, I note that an additional function has been added to protect against an “all rod insertion” event by initiating a scram. This is an event identified during GDA Step 4 and considers the potential for the Class 3 Rod Control and Information System (RCIS) to, as a result of a fault, drive all control rods slowly into the reactor and cause a neutron flux peak event that could challenge the integrity of the fuel. This is reported in the fault studies report.

204. The SSLC uses a de-energise to trip arrangement for the RPS and MSIV functions which means that in the event of a failure in a single division, that division will trip, although two such trips are required for a safety action to be performed. Similarly the load drivers and pilot valve solenoids are normally energised at all times during operation, and a trip demand will result if the output of any two of the four divisions are de-energised. This meets my expectations as this arrangement is used on UK operating reactors and provides adequate resistance to unnecessary trips that can challenge safety, whilst providing a robust tripping system that allows maintenance to be carried out on a division and for legitimate trip to occur even in the presence of a fault in a second division.

205. I found that the SSLC has a variety of testing arrangements, depending on the system. For example, for the RPS a manual or automatic test of the scram pilot valves can be performed, full scram valve test, and test of the input sources to the RPS. I note that the Class 1 application software is designed, where possible, to override a test if a real demand occurs. I have not assessed the test arrangements in detail during GDA, noting that some testing preferences (e.g. which equipment will be tested whilst the reactor is at power and which will be tested during shutdown) will be clarified by the future licensee. Point (a) of AF-UKABWR-CI-011 raised in section 4.2.7 of this report refers to this. I note that Hitachi-GE has produced a testing and maintenance methodology during GDA, and my assessment of this is given in section 4.2.7 of this report.

206. The engineered safety functions use four divisions of sensors and 2oo4 voting to actuate three divisions of mechanical plant using dual redundant logic channels. Both fail safe and fail “as is” functions are deployed, depending upon the safe state of the actuator to prevent a hazard. For example, the primary containment isolation system is fail safe, as isolating the containment reduces risk, whilst the reactor core isolation cooling system is fail “as is”, because of the importance being able to add water to the core during accident conditions. The C&I arrangements meet my expectations

because these are configured in a manner that considers the safety function being performed and the risks associated with different failure states.

207. I note that there is a hardwired control, the SAuxP within the MCR that provides hardwired control, using one division, of the emergency core cooling system equipment. This is required in the event of simultaneous loss of SSLC divisions in conjunction with a large break loss of coolant accident and uses physical switches to activate the panel and actuate equipment. The panel contains indicators which receive signals directly from sensors. This meets my expectations as the hardwired nature of the panel means that this is diverse from the SSLC and PCntlS, and the wiring configuration means that the SSLC cannot interfere with the ability of the operator to actuate equipment once the panel has been activated. Conversely, the wiring configuration of the panel prevents interference with the operation of the SSLC during normal plant operation.

208. I assessed the SSLC documentation (e.g. Refs. 45, 104) to confirm the SFCs have been adequately referenced. Of these SFCs and associated sub-claims sampled, I was able to link each SFC to the fault schedule, through the PCSR and follow the arguments and evidence. I am content that those SFCs sampled provide adequate evidence for the purposes of GDA, and that references to evidence were specific enough.

209. I assessed the SSLC documentation (e.g. Refs. 45, 104) to confirm the SPCs have been adequately referenced. Of these SPCs and associated sub-claims sampled, I was able to link each SPC sub claim to the high level SPCs and follow the arguments and evidence. I am content that those SPCs I sampled provided adequate evidence for the purposes of GDA, and that references to evidence were specific enough.

210. During my assessment I noted SPC 4 claims that C&I systems have an adequate level of redundancy to protect against single failure. Also that the sub claim argument (SPC 4.1.A1) claims that the safety Class 1 SSLC has an N+2 configuration, with a few exceptions. SPC 4.1.A2 states that the primary containment isolation system (PCIS), residual heat removal system primary containment vessel (RHR-PCV) spray and fuel pool cooling and clean-up system (FPC) do not meet the N+2 configuration requirement and references the arguments and evidence why this can be acceptable.

211. I assessed these systems in detail to determine the suitability of the arguments made and the adequacy of the evidence.

212. I found that the PCIS uses sensors in all C&I divisions to detect events that require PCIS actuation, but that the PCIS mechanical arrangement uses two divisions, and the C&I arrangement matches this. Hitachi-GE argue that the PCIS carries out safety functions for infrequent design basis faults and that the probability of the failure of one division whilst another is under maintenance will be lower than $10^{-7}$f/y. I am unable to comment on the adequacy of this argument as the C&I equipment diagnosis, replacement, and return to service times have not been presented during GDA. My expectation is that the adequacy of this arrangement will be confirmed post-GDA during detailed design and after the licensee preferences have been considered.

213. My assessment of the RHR-PCV spray found a similar argument applies. If only two divisions of mechanical plant are required, then the contribution of C&I to unavailability will need to be determined post GDA.

214. My assessment of the adequacy of the C&I arrangement for the FPC system found that there is a number of hours between failure of the FPC system and the onset of a hazardous event. I also noted that there are other systems that can be deployed to cool the spent fuel pool. For these reasons I judge this to be adequate for the purposes of GDA, but note that these arguments are reliant on the failure of the FPC being

detected and action being taken within sufficient time to prevent the hazard being realised. My expectation is that this argument be improved during detailed design to account for the actual arrangements. I see no impediment to additional C&I equipment being deployed if this is found to be necessary.

215. The closure assessment note (Ref. 28) for RO-ABWR-0031 provides further detail of my assessment of the adequacy of the design of the SSLC in respect of C&I redundancy.

216. I also assessed the SSLC sub-systems in respect of separation and independence, and noted that the reactor pressure vessel (RPV) instrumentation to measure coolant level and pressure uses common pressure taps and sensing lines for more than one layer of protection (see Ref. 104). This means that a common cause failure such as plugging of the sensor lines could result in a loss of more than one layer of protection, including the ability of the operators to accurately determine the reactor coolant level.

217. This was raised as a multi-disciplinary RO, RO-ABWR-0061, in the C&I technical area during GDA step 3, also involving fault studies, probabilistic safety assessment, mechanical engineering, structural integrity, reactor chemistry, human factors, internal hazards, external hazards and civil engineering disciplines.

218. Following multi-disciplinary optioneering exercises, Hitachi-GE identified that there were significant risks with having separate instrument sensing lines due to the number of additional ports required in the RPV, and their close proximity in a sensitive area. Hitachi-GE proposed a number of modifications to alleviate the CCF concerns relating to C&I.

219. During my GDA Step 4 assessment I met with Hitachi-GE technical specialists in the C&I area and in conjunction with ONR assessors from other technical disciplines. I also held separate ONR internal technical discussions with the relevant ONR assessors to assess the arguments and evidence being presented in Hitachi-GE submissions, including:

- Measures against Common Cause Failures of Reactor Vessel Instrumentation sensing line (Ref. 139);
- Diversity in detection of fault sequences (Ref. 123);
- Basis of Safety Cases on Safety System Logic and Control System (Ref. 45);
- UK ABWR GDA Supporting Document on Risk Insights on RVI (Ref. 140);
- Reactor Pressure Vessel Instrument System System Diagram (Ref. 124);
- Topic Report on RVI (Ref. 125);
- Investigation of Pipe Whipping Effects Associated with Postulated Rupture of Piping (Ref. 141);
- Topic Report on Internal Hazards Inside PCV (Ref. 142); and
- Pipe Whip and Impact Evaluation Evidence Document (Ref. 143).

220. In order to support the proposed design modifications, Hitachi-GE carried out a PSA sensitivity study. This study was assessed by ONR PSA assessors and the outcome of this review is summarised in the Step 4 UK ABWR PSA Assessment Report.

221. In considering the outcome of the work done by Hitachi-GE, I found the optioneering to have been adequately wide ranging and of sufficient depth. I judge that the arguments and evidence presented demonstrate that the modifications proposed by Hitachi-GE reduce risks so far as is reasonably practicable and have the least impact on the RPV structural Integrity.

222. For these reasons, I closed RO-ABWR-0061. Further detail on the justification and evidence on the design of the RPV instrumentation sensing lines is described in my RO-ABWR-0061 assessment note (Ref. 30).

223. Overall, I judge that the definition of the functional and non-functional requirements of the SSLC is in line with my expectations for the main line of protection of the UK ABWR.

224. In conclusion, my assessment of the SSLC documentation, including claims, arguments and evidence, found this to be adequate for the purposes of GDA. I was able to identify the SPCs and SFCs relating to the SSLC, and in each case to follow these in the documentation to the evidence.

#### 4.2.4.2 Safety Auxiliary Control System

225. The PCSR Chapter 14 (Ref. 39) and the BSC on SACS (Ref. 46) states that the SACS is an independent C&I system (Class 2 to fulfil Category B safety functions) which provides auxiliary functions to the SSLC. The main function of the SACS is to protect the reactor and primary containment vessel in the event of abnormal transients or spurious operation of systems which might possibly impair the reactor safety or in cases where the occurrence of such events is anticipated. SACS is based on the same Class 1 platform used for the SSLC, but I note there is no requirement for SACS to be diverse from the SSLC.

226. The Topic report on the Safety Auxiliary Control System (Ref. 127) provides additional information on the design of the SACS, and states that the SACS development lifecycle will include verification and validation suitable for a Class 2 system, and that SFCs and testing and maintenance will be developed in accordance with IEC 61513. This meets my expectations for this Class 2 system.

227. My assessment has identified that the functions performed by the SACS are categorised appropriately for the functional requirements identified in the fault assessment report (Ref. 42), and that the SFCs have been adequately reflected in the SACS documentation (e.g. Refs. 46, 127), with a description of how each SFC is satisfied.

228. Similarly the SPCs associated with the SACS are specifically identified and evidence provided that these will be met by the design. For example, the redundancy and separation requirements are identified, and outline evidence was provided during GDA that these will be satisfied by the detailed design. The functions provided by SACS primarily require two divisions and this is shown in the submissions provided during GDA.

229. In summary, my assessment of SACS has identified that its functional requirements are adequately identified in the fault schedule, and that the non-functional requirements (e.g. redundancy, diversity) are adequately defined. The evidence provided reflects this. I note that further development of the systems controlled by SACS will be performed post-GDA, but consider that adequate evidence has been presented during GDA that the basis for the design is sound and meets my expectations.

#### 4.2.4.3 Hardwired backup system

230. The PCSR Chapter 14 (Ref. 39) and the BSC on the HWBS (Ref. 47) state that the HWBS is the secondary means of protection under design basis fault conditions for frequent faults together with an additional CCF of a Class 1 SSC, or in the event of CCF of the control and primary safety system, but is also claimed to provide protection against infrequent faults, beyond design basis accidents and severe accidents.

231. The HWBS platform has not been selected during GDA Step 4 but a CAE structure based upon a proposed technology has been presented (Ref. 91). It is a requirement

that the HWBS uses diverse technology to the other main C&I systems (i.e. does not use microprocessors or FPGA's).

232. The HWBS is a Class 2, $10^{-2}$ pfd system that performs Category A safety functions as a secondary line of protection (and can therefore be performed by a Class 2 system). It is separated and isolated from the SSLC. The HWBS receives inputs from 2 sensors in each division and performs 1oo2 twice voting logic to 2 divisions of actuators. This design meets my expectation for an A2 system and is consistent with my expectations for reliability and single failure criterion.

233. The Basis of Safety Cases on Hardwired Backup System (Ref. 47) states that the HWBS performs reactivity control (standby liquid control, recirculation pump trip, feed-water stop, and alternative rod insertion), fuel cooling (reactor depressurisation control facility and Flooder system of specific safety facility), and long term heat removal (filtered containment venting system and hardened vent line) functions.

234. Hitachi-GE claim that support systems for the HWBS (Electrical Power System and Heating and Ventilating Air Conditioning and Cooling System (HVAC)) that are controlled by the HWBS are separated from systems that are controlled by the SSLC.

235. The HWBS claims and sub-claims are stated in the Basis of Safety Cases on Hardwired Backup System (Ref. 47). My assessment identified that each top level SPC has been broken down into sub-claims (and in some cases sub-sub-claims), and that arguments and evidence have been identified uniquely. My sampling found that evidence clearly refers to specific sections of documents (including outside the C&I area), and that these documents contain the evidence claimed. For example, I followed the claim that the support systems are separated from systems controlled by the SSLC, and found adequate evidence that this is the case in Ref. 90. However, I found that the text in the Topic Report on Hardwired Backup System (Ref. 90) has limited references to which evidence the text is intended to fulfil (i.e. the electrical power supply section does not state this is the evidence for the relevant SPC). Nevertheless, I consider referencing is adequate for the purposes of GDA. My expectation is that this will be improved when detailed design is undertaken and the safety case is further developed.

236. I note that the hydraulic control units which insert the control rods are actuated by both the SSLC and the HWBS, but that the two systems use different pilot valves (the SSLC de-energise to actuate and the HWBS energise to actuate). I find this to be acceptable as this maintains the electrical separation between both systems.

237. I assessed the HWBS documentation (e.g. Refs. 47, 91) to confirm the SFCs have been adequately referenced. Of the SFCs and associated sub-claims I sampled, I was able to link each SFC to the fault schedule, through the PCSR, and follow the arguments and evidence. I am content that those SFCs I sampled provided adequate evidence for the purposes of GDA, and that references to evidence were specific enough.

238. My assessment of the HWBS documentation found that the functions of the HWBS have been adequately documented, and references other systems where necessary to demonstrate separation and diversity. For example, the HWBS that controls the ARI provides a diverse means of inserting the control rods from that of the SSLC.

239. I found the RDCF and the FLSS functions provide a diverse injection system if the Class 1 ECCS should fail. These functions are shared with SA C&I system, located in the Backup Building (B/B) and can be controlled from B/B control panel if necessary. The control of these function can be switched to SA C&I system via transfer switches located at the B/B. This design meets my expectation for defence in depth, diversity and diversity in detection of fault sequence including severe accident conditions.

240. The HWBS shares certain functions with the SA C&I system which are located in the Backup Building. Therefore, some HWBS equipment is required to sustain severe accident conditions as described in the Accident Management Guideline (AMG) (Ref. 131).

241. During my assessment, I identified that both divisions of the hard wired backup panels are adjacent to each other and both divisions of the HWBS are routed through the same service tunnel (Ref. 90). I raised RQ-ABWR-1391 requesting evidence that hazards will not affect both divisions at the same time. Hitachi-GE's response (Ref. 128) stated the combined frequency of the infrequent internal hazards and the loss of the Class 1 SSLC is considered to be a low probability. Also, should a frequent internal hazard (e.g. a fire) prevent the HWBS delivering its safety function and also causes a frequent Design Basis fault (an Initiating Event), appropriate measures will be implemented for the relevant HWBS components to prevent the simultaneous loss of the HWBS divisions. The RQ response gives a specific commitment that if it is found necessary, a study to determine appropriate measures will be implemented post-GDA. I consider this is adequate, as during GDA there is insufficient information to determine whether a design change will be necessary, and this information will not become available until detailed design.

242. I conclude that although Hitachi-GE has not made a HWBS technology decision during GDA, sufficient information has been submitted that has enabled an assessment to be carried out. My assessment has concluded that the principles for the design of the HWBS have been established, that the functionality has been suitably identified, and that the design information is sufficiently detailed, supported by the safety case, to demonstrate the design is adequate for the purposes of GDA.

#### 4.2.4.4 Severe Accident C&I System

243. The PCSR Chapter 14 (Ref. 39) and the BSC on SA C&I system (Ref. 48) state that the SA C&I system is used to mitigate the consequences of severe accidents. Specifically this:

- provides key indications of the plant state from SA qualified instrumentation to enable effective operator actions to be taken;
- allows the operator to utilise available mechanical equipment to provide fuel cooling, long-term cooling and containment functions; and
- provides mobile equipment which can be connected to the plant to provide an additional means of achieving fuel cooling, long-term heat removal and containment functions.

244. My assessment of Hitachi-GE submissions (e.g. Refs. 39, 48, 122) confirmed that the SA C&I is an independent C&I system located in the B/B, is based on hardwired relay logic to implement Category B and C safety functions, is designed according to the safety lifecycle defined in IEC 61513, and to meet the recommendations of the Accident management Guideline (AMG).

245. In respect of connection with other C&I systems, I found that the SA C&I system shares some sensors and mechanical equipment with the HWBS, but that the SA C&I is disconnected during normal operation and cannot interfere with the HWBS operation. Transfer switches are used to activate the SA C&I. In addition to fixed SA C&I equipment, separate independently controlled mobile equipment with its own embedded C&I components provides a further layer of mitigation during SA conditions.

246. In summary, I judge that Hitachi-GE has provided sufficient information on the design of the SA C&I system during GDA Step 4, and that this is adequate, noting that further detail will be developed post-GDA.

#### 4.2.4.5 The Plant Control System

247. The PCSR Chapter 14 (Ref. 39) and BSC on PCntlS (Ref. 49) states that the PCntlS is used to control and maintain the plant condition during normal operation. The PCntlS is directly classified as a Class 3 system, with a claimed failure frequency of $10^{-1}$ ffpy.

248. The PCntlS consists of the reactor power control, the reactor water level control and the reactor pressure control, the key functions include the recirculation flow control system (RFC), rod control and information system (RCIS), electro-hydraulic turbine control system (EHC), feedwater control system (FDWC) and automatic power regulator (APR). The control system contributes to nuclear safety by keeping the reactor within the intended operational boundaries, avoiding demands being placed on the protection systems. My assessment confirmed this is consistent with fault analysis (Ref. 42).

249. I assessed the PCntlS documentation (e.g. Refs. 49, 120) to confirm the SFCs have been adequately referenced. Of the SFCs and associated sub-claims I sampled, I was able to link each SFC to the PCSR, and follow the arguments and evidence. I am content that those SFCs I sampled provided adequate evidence for the purposes of GDA, and that references to evidence were specific enough.

250. I assessed the PCntlS documentation (e.g. Refs. 49, 120) to confirm the SPCs have been adequately referenced. Of the SPCs and associated sub-claims I sampled, I was able to link each SPC sub claim to the high level SPCs, and follow the arguments and evidence. I am content that those SPCs I sampled provided adequate evidence for the purposes of GDA, and that references to evidence were specific enough.

251. I assessed the evidence provided and confirm that the PCntlS is a system that is independent of the C&I systems performing protection functions, and that it cannot influence these. Similarly the Class 3 platform, HIACS, uses microprocessor technology which is diverse to the Class 1 and Class 2 platforms, and meets my expectations on diversity.

252. During GDA Step 4 it was identified that a failure in the PCntlS RCIS function could result in the control rods being spuriously driven into the core slowly, resulting in excessive local power peaking. ONR raised RO-ABWR-0077 requesting Hitachi-GE to develop a safety case to demonstrate an adequate protection against this. Hitachi-GE submitted an analysis and optioneering study of all control rods insertion faults (Ref. 82) and their potential mitigation (an additional SSLC-driven A-PPRM scram signal). This additional safety function was inserted into the fault schedule (Ref. 42), was assessed by the FS inspector (Ref. 138), and was found to be acceptable. I judge that Hitachi-GE has identified adequate C&I countermeasures to this potential fault that will be effective and implementable. I consider it acceptable that these will be developed further post-GDA.

#### 4.2.4.6 Reactor/Turbine Auxiliary Control System

253. The PCSR Chapter 14 (Ref. 39) and the BSC on Basis of Safety Cases on Reactor / Turbine Auxiliary Control System (Refs. 50, 129) states that this provides control for the turbine, the generator and their major auxiliaries such as cooling water. The majority of the sub-systems are directly classified as Class 3, or are not classified, in line with the SCDM (Ref. 38). This system is implemented on the HIACS platform.

254. My examination of the evidence provided in Refs. 50 and 129 found the methodology for the identification of the functional requirements SFCs (where relevant) of the system and its sub systems to be adequate, and the identification of non-functional requirements (SPCs) to be suitably documented.

255. I consider sufficient information has been provided during GDA to provide confidence that the design approach established will meet UK regulatory expectations post-GDA.

#### 4.2.4.7 The Plant Computer System

256. The PCSR Chapter 14 (Ref. 39) and BSC on PCS (Ref. 51) states that the PCS provides monitoring, recording and display functions.

257. My assessment identified that the Class 3 PCS is not used to directly control the plant. I have not assessed the communication between the PCntlS and PCS in detail during GDA. I note that the PCS is not connected to higher class systems, and does not share resources (e.g. electrical supplies) with them, so cannot influence them.

258. The PCS drives the Plant level Flat Displays (PFD) for current, trend and related information. The PCS displays via control room displays and has its own operator interface. It provides data logging and alarm functions. I consider this arrangement is adequate and that it provides independent monitoring functions and backup monitoring facility in event of the HMI failure.

259. The PCS is capable of transmitting plant data to the main office and off-site location (one way communication only) via the site host computer in event of an emergency. This allows emergency technical support if required. I consider this arrangement is adequate and would support emergency response.

260. Based on the above evidence and the detail given by Hitachi-GE, I judge the design of the PCS is adequate.

#### 4.2.4.8 Support systems

261. During GDA Step 3 Hitachi-GE submitted the BSC on HVAC (Ref. 163), and ONR identified that there was insufficient detail of the HVAC design in order to carry out a meaningful assessment. RO-ABWR-0075 was issued, led by ONR Mechanical Inspectors, requesting further evidence to demonstrate the robustness of the HVAC design for UK ABWR and that potential risks could be reduced so far as is reasonable practicable.

262. During GDA Step 4 Hitachi-GE revised the safety case for HVAC. I assessed the latest submission of the BSC on HVAC (Ref. 126) and confirm that:

- categorisation and classification of the HVAC has been suitably assigned and that it is consistent with the categorisation and classification of the C&I systems which it supports;
- different classes of HVAC are adequately segregated between different classes (i.e. Class 1, 2 and 3); and
- the auxiliary services that support components of systems important to safety are considered part of that system, and adequately Categorised and Classified.

263. Based on the evidence provided, I judge the design of the HVAC provision for C&I systems is adequate for the purposes of GDA and meets my expectations.

264. Hitachi-GE has not completed the detailed design of the electrical power system during GDA step 4. However, by assessing the relevant C&I documentation (e.g. Refs. 39, 44, 45, 46, 47, 49) I was able to confirm, using a sampling assessment, that the Categorisation requirements for the electrical power supplies for the C&I systems have been identified and that these are the same Classification as the C&I systems they support. Also, I note that where there is a requirement for the C&I system to be diverse from others, this requirement extends to support systems.

265. For this reason, I judge the requirements of the electrical power systems that support the C&I systems to be adequate, noting that further work will be done post-GDA.

#### 4.2.4.9 Other systems

266. The PCSR chapter 14 identifies a number of other C&I systems that are used in the UK ABWR, including the traversing in-core probe, area radiation monitoring system, the process radiation monitoring system, radiation waste systems, and embedded C&I systems such as those in the reactor building overhead crane (RBC) and the fuel handling machine (FHM). My expectation is that the full justification of these systems and their interconnection with other C&I systems will be completed post GDA as their design develops and the definition of their functional requirements finalised.

267. In GDA, I assessed the C&I aspects of the outline design of the RBC, and FHM. Hitachi-GE submitted a Topic Report on Fault Assessment for SFP and Fuel Route (Ref. 43) this document describes the fuel route and the equipment associated with this, including the fuel handling machine (FHM), the reactor building overhead crane (RBC) and the spent fuel pool (SFP) instrumentation.

268. The report covers the operation and interaction of the equipment with other equipment and surrounding structures. For example, the FHM is used to remove and replace the Reactor Internal Pumps (RIPs) which can involve a complex set of movements to navigate around the reactor well, RPV flange and into the correct location using both manual and automatic operations.

269. Similarly, the RBC can perform a range of different operations and has to avoid interaction between the crane and load and fixed and moveable structures over a range of different equipment configurations. A specific requirement is for the RBC to handle a cask containing spent fuel from the SFP, through various operations around the operating deck, and to lower this to ground level, although the RBC also performs a number of other lifts in and around the RPV and associated equipment.

270. The Topic Report on Fault Assessment for SFP and Fuel Route (Ref. 43) identifies bounding faults for the SFP, and fuel route, and presents a fault schedule for the associated equipment, including the FHM and the RBC. This identifies Category A safety functions that are performed by the FHM and RBC and identifies a requirement for these to be classified as Class 1. I note that this also places a requirement for Class 1 protection on the FHM and RBC (e.g. High Integrity Controllers and Input Devices (A1, automatic), and Main hoist emergency brakes (A1, automatic)).

271. The topic report also provides a high level schematic of the FHM and RBC mechanical, control and protection arrangement, showing a range of control and protection equipment, and a Failure Modes and Effects Analysis (FMEA) of systems and components.

272. This identifies a range of hardwired and software features to prevent faults or human error from leading to impact or loss of control. This includes "…Hardwired limit switches prevent collision with the SFP walls & cask pit walls. The signals from these limit switches feed into software logic which ensures the protection only acts when the hoist is within a specific cross travel range….". No further information is provided on the categorisation of the safety function for this, so it is not possible to confirm the adequacy of the arrangement during GDA. However, based on the text presented, I have concerns regarding the adequacy of using software to achieve what appears to be a high reliability safety function.

273. I therefore raise an Assessment Finding relating to the complexity and suitability of the proposed arrangement – see below.

274. I also sampled for assessment the outline design of the RBC to handle a cask containing spent fuel from the spent fuel pool, through various operations around the operating deck, and to lower this to ground level. This is described in a separate assessment report (Ref. 136). The outcome of my assessment was that I identified a number of concerns regarding the end-to-end testing of certain components (e.g. the centrifugal overspeed switch), the feasibility of qualifying certain components at the required classification (e.g. laser scanner for ledge protection), the completeness of the analysis (e.g. a potential shortfall in the capture of a fault or its consequences), and the complexity of the design outlined.

275. During GDA the potential operations required of the RBC and associated equipment have not been fully identified, as these will depend upon the requirements of the future licensee. However, my assessment has identified a number of concerns which need to be addressed early in the UKABWR licensing phase. For this reason I raise an assessment finding.

> *GDA Assessment Finding: **AF-UKABWR-CI-018** - Whilst the principles for the C&I of the reactor building overhead crane and fuel handling machine were outlined in GDA, detailed design will depend on the licensee's choice. Based on the information available, ONR has identified a number of challenges which should be considered as part of the requirement specification and design of the systems.*
>
> *The licensee shall ensure that during the detailed design of the reactor building crane, fuel handling machine, and associated equipment, that optioneering and safety analyses adequately consider all functional and non-functional requirements, including those associated with all operational and proof test requirements, to ensure that a demonstration of adequate risk control can be achieved. The optioneering and analysis to include, but not to be limited to;*
>
> *a. Identification of all operational requirements, including those associated with non-reactor operations.*
>
> *b. Application of the hierarchy of controls to avoid reliance on complex systems, where reasonably practicable.*
>
> *c. The feasibility of end to end testing of all safety devices and systems (e.g. centrifugal switches).*
>
> *d. The feasibility of qualifying components to meet safety functionality requirements and for adequate justification to be provided (e.g. complex devices such as laser scanners).*

276. I note that during GDA all the fuel handling machine operational requirements may have not been identified, as many of these arise from site specific and licensee requirements. I have therefore not assessed submissions relating to this during GDA.

#### 4.2.4.10 C&I systems located in the Backup Building

277. During GDA Step 3 ONR raised RO-ABWR-0026 (Ref. 14) requesting Hitachi-GE to provide high level descriptions of the C&I systems located in the Backup Building.

278. During GDA Step 4, Hitachi-GE submitted a description (e.g. Refs. 39, 48, 122) of C&I safety systems in the Backup Building to manage infrequent design basis events, beyond design basis faults, and severe accidents. These systems are the Hardwired Backup System and the Severe Accident C&I System.

279. I assessed the design of the shared functions (e.g. flooding system of specific safety facility (FLSS), reactor depressurization control facility (RDCF), filtered containment

venting system (FCVS) and support systems) between the HWBS and the SA C&I system, noting that in the event of severe accident conditions, the control from the HWBS to SA C&I system will be switched via transfer switches located in the Backup Building (e.g. SA C&I SFC 5-4.1).

*280.* Transfer switches are used to switch control from the HWBP (located in the MCR) to the BBCP (located in the B/B). Ref. 47 states these switches block indication on the HWBP and permit commands and indication on the BBCP. This allows operators to determine when to activate the RDCF and to monitor and confirm the operation has been successful. Hitachi-GE has stated that the detail of transfer switches will be further developed post-GDA. I consider this to be adequate for the purposes of GDA as I judge that the recommendations made in the ONR Chief Inspector's final report, "Japanese earthquake and tsunami: Implications for the UK nuclear industry" (Ref. 130), will be satisfied by this arrangement.

281. Based on the evidence provided during GDA Step 4, I judge the proposed arrangement of the Backup Building C&I system to be adequate for GDA. I understand there will be further development of the design of the Backup Building and the transfer switches operation and its design post-GDA.

#### 4.2.4.11 Conclusion of C&I system assessment

282. My assessment of the Hitachi-GE UK ABWR C&I GDA submissions has identified that a number of different system arrangements are documented that perform a wide range of safety and non-safety functions. My sampling assessment focussed on safety systems and I found the functionality of these is determined adequately from the fault schedule, the safety case clearly identifies the design principles, and that these are reflected in the design documentation presented during GDA (e.g. interconnections are designed to prevent lower class systems from influencing higher class systems). Similarly I found that the system design documentation agrees with the Basis of Safety Cases on C&I architecture submission (Ref. 44) and that the documentation clearly states support system safety claims. I found the systems to be adequately documented for the purposes of GDA, but note that additional work will be required post-GDA to ensure that detailed design requirements are met by the systems' design.

283. In summary, I am content that an adequate safety case has been provided for the UK ABWR C&I systems, for the purposes of GDA.

### 4.2.5 Human machine interfaces

284. HMI supports operator understanding of the state of the reactor and its auxiliary systems, and enables timely and effective interventions to perform routine actions during normal operations and, when necessary, under accident conditions. It is therefore necessary for the HMI to operate with an adequate reliability that supports the requirements placed on it by the safety analyses.

285. HMI can also be a hazard to the correct operation of the reactor through inadvertent actuation of controls due to human error, spurious actuation due to a C&I or electrical fault, or through interference between connected systems.

286. RO-ABWR-0028 was raised earlier in GDA because the HMI functionality had not been established and used touch screen technology. Also, the design processes used for the Class 1 HMI had not been adequately described and an adequate CAE structure was not in place.

287. Therefore, I assessed the adequacy of the HMI safety case, the ability of HMI to perform the functions required at the required reliability and to prevent spurious actuation, and the measures to prevent interference between different classes of HMI.

288. The PCSR chapter 21 (Ref. 41) provides an outline of the requirements and safety function and safety property claims for HMI, including control locations, requirements on different systems, assumptions and limits and conditions of operation, and ALARP justification.

289. The UK ABWR is designed for safety actions to be taken automatically, placing little requirement on the operators or other personnel to take safety actions except under specified conditions. However, there are requirements for operators and other personnel to monitor the status of the plant, to perform actions to control the normal operation of the reactor and auxiliary equipment, to perform actions that facilitate maintenance and testing of equipment, and to take action in the event of failure of automated systems.

290. The HMI designs have not been completed during GDA. Information relating to HMI Categorisation and Classification, design basis, functional design, and the majority of functional specifications for most systems has been provided during GDA, as well as the concept layout.

291. The suitability of monitoring and control requirements in relation to what information needs to be displayed and what controls need to be present is out of scope of this assessment. However, I have assessed the suitability of the equipment to perform those monitoring and control operations identified during GDA, with the intent of confirming the adequacy of HMI and its supporting systems.

292. The control locations are areas used for monitoring, decision making, action, and confirmation. Table 4 sets out the control locations where HMI is situated:

| Control Location | Use | Main HMI's present |
|---|---|---|
| Main Control Room (MCR) | Monitoring and operation in all circumstances except when the MCR is uninhabitable | • Main Control Console (MCC);<br>• Wide Display Panel (WDP);<br>• Safety Auxiliary Panel (SAuxP);<br>• Hardwired Backup Panel (HWBP) |
| Remote Shutdown System Panel room (RSSR) | Monitoring and operation when MCR is uninhabitable | • Remote Shutdown Panels (RSPs) |
| The Back-up Building Control Panel Room (BBCR) | Monitoring and operation during fault conditions, particularly Severe Accident conditions when the MCR and RSSRs do not provide the required functionality or when it is not feasible for personnel to remain in the reactor building. | • Backup Building Control Panel (BBCP) |

| Control Location | Use | Main HMI's present |
|---|---|---|
| Radioactive waste building Rw/B MCR | Monitoring and control of the C&I systems and plant associated with the radioactive waste facility | Not covered during GDA |
| Local control Locations | Control and monitoring for other specific SSCs that are not linked to the main C&I systems throughout the plant | Not covered during GDA |

**Table 4.** Control locations, HMI's, and their purpose.

293. The PCSR Chapter 14 (Ref. 39) and Basis of Safety Cases on Control and Instrumentation Architecture (Ref. 44) show the HMI for the main C&I systems, the connectivity of the systems, and the method of interconnection (i.e. networked or hardwired, bidirectional or mono directional information flow).

294. The Basis of Safety Cases on Overall Human-machine Interfaces (Ref. 52) describes the requirements for the Classification of the HMI, referencing the principles from which the criteria for the Classification of the HMI are derived, namely;

- classification of the system that the HMI is connected to;
- the reliability requirement of any human based safety claim (HBSC) that the HMI is associated with; and
- the importance of tasks (primary or backup/additional measures).

295. I performed an assessment to confirm that this principle has been followed and that the HMI classification matches the system to which it is connected.

#### 4.2.5.1 HMI Classification

296. The Basis of Safety Cases on Overall Human-machine Interfaces (Ref. 52), Basis of Safety Cases on Main Control room Human-machine Interface (Ref. 53), Basis of Safety Cases on Remote Shutdown System Human-machine Interface (Ref. 54), and Basis of Safety Cases on Backup Building Human-machine Interface (Ref. 55) describe the HMI associated with each control location and its classification.

297. The BSC on C&I architecture, figure 5.1.2-1, shows the classification of the systems and the HMI associated with those systems. In each case the classification of the HMI matches that of the system to which it is connected (i.e. the HMI for the SSLC is Class 1, for the HWBS, SA C&I, and the SACS are Class 2, and for the PCntlS, Reactor and Turbine Auxiliary System, and the plant computer system are Class 3). The classification matches my expectations in respect of the Categorisation and Classification identified for those systems identified in the fault schedule (Ref. 42).

298. Hitachi-GE has identified the need for certain systems to have a redundant architecture and be divisionalised to ensure adequate reliability and continued ability to respond to safety demands, even in the event of a failure in one part of the system. It is important that where separate divisions are relied on to provide adequate risk control, that this is reflected in the architecture of the HMI, and that there is adequate separation between them.

299. The Basis of Safety Cases on Overall Human-machine Interfaces (Ref. 52) states that the SSLC, HWBS and SACS all have redundant architectures. I have confirmed that

there is to be a separate HMI for each division of these systems and that the divisions are not connected in any way (e.g. the digital communication bus between each division of the SSLC and its HMI is electrically separated from the digital communication bus of the other divisions). I am therefore satisfied that a fault or failure in one division of either the system or HMI will not directly affect the correct operation of any other division. Similarly, an incorrect command or actuation request cannot affect more than one division.

300. A fundamental safety principle is that lower Class systems do not affect higher Class systems. It is also important to confirm that the technology used to implement each HMI is suitable for the system to which it is connected, and that the principle of diversity between the three main layers of protection has not been compromised. I therefore sought evidence of the technology used for each HMI and any interconnection between HMI of different Classes.

301. By reviewing the relevant submissions (i.e. Refs. 44, 52 - 55) I was able to confirm that there is no interconnection between the HMI of different Classes and therefore that lower Class HMI cannot influence higher Class systems.

#### 4.2.5.2 Suitability of HMI technology

302. I was also able to confirm that the technology used to implement the HMI's also matches my expectations, as described below.

303. For example, the HMI for the hardwired backup system is described (Refs. 52, 53, 47, 91) as using hardwired components for both indicators and controls. I note that the platform for the HWBS has not been selected during GDA but that an example technology has been described. This meets my expectations with regard to the hardwired design of the controls and indicators. I am satisfied that in the event of this technology not being selected, that there are a number of other feasible options that will meet the objectives of ensuring the HWBS HMI technology is diverse from that of other HMI, and that this uses non-programmable components. However, I have raised this as point (d) in AF-UKABWR-CI-014 (see Annex 5).

304. The need for common cause failures in the C&I to be avoided places a requirement for the Class 1 SSLC to be diverse from the technologies used in the HWBS (hard wired) and the PCntlS (microprocessor). The SSLC HMI has to similarly avoid the potential for common cause failure.

305. The detailed design for the SSLC HMI has not been completed during GDA, but enough information is available for me to assess whether the technology proposed for the Class 1 SSLC HMI is sufficiently diverse from the other HMI. My review of the relevant submission (Ref. 93) has identified that the SSLC HMI proposes to use a flat panel display and the same FPGA technology used for the Class 1 SSLC platform. I am satisfied that the design requires that the Class 1 SSLC HMI platform does not contain microprocessor technology and that the proposed development process for configuring the FPGA matches that of the SSLC platform and is adequate for Class 1 (i.e. it satisfies the relevant ONR SAP's, TAG's, and international standards), as discussed in section 4.2.3 of this report. I am also satisfied that Hitachi-GE has demonstrated the design of the Class 1 SSLC HMI platform is feasible without the use of microprocessors. My expectation is that post-GDA the licensee will continue to develop this outline design and will demonstrate this meets relevant standards and guidance.

306. I note that, following an optioneering exercise, Hitachi-GE does not propose that the Class 1 HMI uses touchscreen technology. Hitachi-GE has proposed a replacement for the touchscreen technology with a screen navigation system based on hardwired technology. I am satisfied that the design that has been proposed for the Class 1 HMI

screen navigation will not result in a reduction in diversity between this HMI and that for the HWBS controls. The use of a hardwired device to enact commands is important as it reduces the risk that a fault in the Class 1 HMI system will send an uncontrolled or unexpected command to the SSLC.

307. I was concerned that the technology proposed for the Class 1 SSLC HMI would not have the capacity and capability required to provide the features and facilities required. I therefore reviewed the Functionality of Class 1 HMI for the SSLC (Ref. 94), to confirm that the functionality of the display had been identified and understood. This describes the process by which the functionality of the Class 1 HMI has been established, including task analysis and allocation to HMI components. I judge that this is adequate to ensure that the functionality of the Class 1 HMI has been understood, and that the allocation to HMI has been established. Similarly the submission Safety Concept for vCoss/NCFS-1 Platform (Ref. 86) describes how the components of the NCFS-1 platform will be configured to implement the functionality required. Furthermore this submission analyses the consequences of the NCFS-1 platform failure on the display presented to the operator. This gives me confidence that the capacity and capability of the Class 1 HMI will be adequate when detailed design has been completed. I also judge that the Class 1 HMI will be capable of indicating a fault to the operator.

308. During GDA I focused on higher class systems, and therefore did not assess in detail the adequacy of the HMI design of lower class systems such as the PcntlS and the Plant Computer System. However, I did confirm that the HMI associated with these systems is not connected to higher class systems, and therefore cannot adversely influence them.

309. Hitachi-GE has produced a safety case that uses a Claims, Arguments, Evidence (CAE) structure and Safety Property Claims (SPCs) to demonstrate that the safety requirements of the HMI design (e.g. diversity, separation, redundancy) have been met by the design. I have sampled these, and am content that the safety properties have been correctly identified and that there is sufficient evidence that these have been met.

310. My assessment of the submissions to support the closure of RO-ABWR-0028 (Ref. 16) during GDA Step 4 found that HMI functionality had been clarified, separation of safety classes has been demonstrated, the selected technology (including the avoidance of touchscreen technology for Class 1) is appropriate for the system classification, and that measures to prevent fault propagation, provide appropriate design processes, and CAE structure are adequate. I recorded my assessment of these in an assessment note (Ref. 25), in which I concluded that these issues had been adequately resolved, and closed RO-ABWR-0028.

311. My assessment of the proposed design of the HMI is that during GDA Step 4 the design has been adequately advanced to allow assessment, and that this satisfies the relevant SAP's, TAG's, and meets appropriate international standards. The safety case is sufficiently developed for the purposes of GDA and is structured to allow further development and refinement during the site-specific phase of the UK ABWR.

312. In conclusion, I judge that Hitachi-GE has made a suitable demonstration during GDA of the adequacy of the C&I aspects of the HMI.

#### 4.2.5.3 Alarms

313. Hitachi-GE submitted a number of documents to describe how the requirement for alarms would be identified, how they would be classified, and what equipment would be used to display alarms.

314. For example, the Alarm Processing and Presentation Strategy (Ref. 95) describes a methodology for the identification of alarms that may be associated with different types

of equipment (e.g. mechanical, electrical, and C&I equipment), prioritisation, rationalisation, and different alarm types. The Alarm Basic Design Specification (Ref. 96) describes an approach to the classification of alarms, and how these alarms may be realised. Figure 3.4-1 of Ref. 96 shows a range of alarm equipment such as a stand-alone annunciator, indicators, flat panel displays, and logging devices. It also shows higher class equipment (e.g. the Class 1 SSLC and Class 2 SACS) providing alarm information to the Class 3 plant data network using one-way communication to avoid the potential influence of the lower class plant data network on the higher class systems.

315. I have noted that these reports refer to relevant standards and guidance (e.g. IEC 61226, IEC 61513, EEMUA 191), but are generally conceptual in nature and don't present enough detail for an adequate assessment to be carried out within GDA. I am therefore not able to present a finding on the adequacy of the HMI in respect of displaying and managing alarms. However, I note that the majority of alarms are displayed by lower class systems and am of the opinion that these are likely to have the capacity and capability to perform the necessary processing and display functions to ensure that objectives relating to alarms (e.g. prioritisation, suppression) can be met. I note that a stand-alone alarm annunciator is shown for alarm indications from the Class 1 SSLC. No further detail has been given during GDA, and my expectation is that a stand-alone annunciator should be capable of displaying alarms with the necessary reliability and also has the necessary electrical isolation to avoid the potential for the Class 1 SSLC to be influenced. For this reason I raise AF-UKABWR-CI-017 (see below).

316. During the work to close out RO-ABWR-0061, Hitachi-GE supplied two documents that describe the design of the Excess Flow Check Valve (EFCV) on each of the Reactor Vessel Instrumentation (RVI) sensing lines (Refs. 112). These documents show that the alarm contacts for the EFCV are normally open.

317. My expectation is that alarm contacts would be normally closed on the basis that any failure of the contact or wiring would be revealed by the sounding of the alarm. I raised this in a technical meeting with Hitachi-GE who were of the opinion that alarms with normally closed contacts would present a risk of alarm flood if the power supply failed and that this is undesirable.

318. I have subsequently confirmed that good practice in the UK is that alarm contacts are normally closed, and that the potential for alarm floods can be managed by using redundant power supplies and the suppression of alarms in the event that power supply failure occurs. I therefore raise an assessment finding below.

319. In addition, during GDA the C&I design of the alarm systems was not clearly established as the requirements for the C&I aspects of alarms were not identified. I note that further requirements will arise from the licensee post-GDA, and that this may significantly influence the architecture and functionality of alarms. The importance of establishing the alarm requirements and architecture early post-GDA to ensure the overall C&I design remains adequate is such that I raise an assessment finding relating to this.

> *GDA Assessment Finding: **AF-UKABWR-CI-017** - In GDA, Hitachi-GE provided outline information describing alarms. ONR's expectation is that as more detailed design information becomes available the design is adequately substantiated, in particular considering claims and engineering requirements.*
>
> *The licensee shall:*

*a. Identify the engineering requirements for each alarm considering appropriate factors (such as impact on risk, aversion to alarm flood, fault detection, human factors).*

*b. Justify the adequacy of the alarm design against the requirements (including the use of normally open or normally closed contacts), considering relevant good practice in the UK and relevant guidance.*

*For further guidance see the Technical Observations for AF-UKABWR-CI-017 in Annex 5.*

**Transfer of control location**

320. During my assessment of the HMI architecture and control locations (Refs. 52 - 55), I noted that it is necessary for operators to be able to continue to monitor reactor parameters and to perform actions under a range of different failure, fault, and accident conditions.

321. The conditions that may result in the operator changing to different workstation or control locations include failure of C&I equipment, the MCR becoming uninhabitable, or a severe accident coupled with the MCR becoming uninhabitable.

322. A number of actions result from the conditions described, including movement from one control desk to another, or movement of operators to another room or building.

323. I have assessed the C&I arrangements for the transfer of control from one control desk to another and from one room/building to another, reviewing the safety claims arguments and evidence relating to the transfer of control.

324. I have examined the evidence provided in the HMI and other documentation, and judge that an adequate outline demonstration has been made that the transfer switches will enable adequate transfer of reactor monitoring and operation.

325. I noted that the HMI documentation supplied by Hitachi-GE did not describe how movement from one control location to another (MCR/RSSR, MCR/BBCR) could be prevented by hazards affecting the transfer switches, or their immediate location, and what design measures are in place to ensure access to displays and controls in a range of events.

326. I therefore raised RQ-ABWR-1470 (Ref. 37) requesting further information on hazards affecting transfer switches in conjunction with the internal hazards assessor. This requested information on what IH considerations were included in both the design of the transfer switches and their location, covering event types, failure modes of transfer switches, and justification of adequacy.

327. The Hitachi-GE response to this RQ (Ref. 113) referenced the internal hazards assessment (Ref. 97), noting that pipes and valves for the makeup water purification system had been removed from the RSSR, removing a number of hazards associated with these items, leaving fire as the remaining internal hazard. Failure modes induced by internal fire at the RSSR and BBCR were identified by the Fire PSA (Ref. 98). The contributions of internal fires originating at the RSSR and BBCR to the overall fire risk were quantitatively studied by the Fire PSA (Ref. 162).

328. The response also describes the potential consequences of fire on the transfer switches, including spurious actuation and loss of controls/monitoring ability. Multiple spurious operations have been analysed in the document “Multiple Spurious Operation (MSO) Scenario Identification Report” (Ref. 99) and the response describes the consequences of the loss of control and/or monitoring for each location.

329. Hitachi-GE states that automatic functions will not be affected by either event because 2oo4 voting applies, and that manual operation of two divisions will remain unaffected. Hitachi-GE also state that SA C&I and HWBS could both be affected, but that this is protected by the independent Class 1 system, and loss of both these systems is assumed in the safety analysis.

330. I note that there are SPCs relevant to the arguments made in the RQ response, claiming the independence of relevant C&I systems, and that adequate evidence has been presented during GDA to confirm these will be satisfied by the detailed design. I therefore judge this RQ response to be acceptable.

331. Detailed information on the transfer switch design and implementation has not been presented during GDA. Whilst, as described above, an adequate safety case has been presented for the purposes of GDA, I note that the transfer switches are a sensitive area for risk management because many sensor and actuator cables from a wide range of systems and number of layers of protection are likely to be present in a small physical area, hence placing a particular focus on hazard analyses. I also note the relevance of human factors in determining the suitability of the C&I transfer switch design. For this reason I raise assessment finding AF-UKABWR-CI-016.

> *GDA Assessment Finding: **AF-UKABWR-CI-016** - The GDA C&I safety case relies for a number of functions on transfer switches (e.g. for actuator selection and transfer of command to a different control location). Although the principles for these transfer switches are acceptable, when developing its detailed design additional justifications are expected, in relation to classification, robustness and operation.*
>
> *The licensee shall demonstrate the suitability of the detailed C&I design of transfer switches, to address the following:*
>
> *a. Suitability of classification.*
>
> *b. Failure characteristics.*
>
> *c. Resistance to hazards (including physical and security hazards).*
>
> *d. Human factors in operation.*
>
> *e. Time to operate relative to timescales for fault scenarios.*
>
> *For further guidance see the Technical Observations for AF-UKABWR-CI-016 in Annex 5.*

#### 4.2.5.4 Conclusion of HMI assessment

332. In conclusion, I am content that a suitable demonstration has been made in GDA that adequate control and monitoring of the important reactor systems will be possible on the UK ABWR, and that this can be maintained during a number of different events. I found the arrangements to respond to faults and to move control and monitoring to a different location to be adequately developed for the purposes of GDA, but note that additional design and substantiation work will be required post-GDA.

### 4.2.6 Smart device justification

333. A smart device is a complex electronic component controlled by a microprocessor or complex hardware logic, whose functions are limited and cannot be fundamentally changed after manufacture. By limited functionality it is meant that the external functionality seen by the user appears to have limited complexity. However, the

internal complexity within the device is likely to be significant. In most cases, smart devices are commercial off-the-shelf (COTS) designs, or use COTS components, not originally developed to nuclear standards. A more comprehensive description of a smart device is provided in clause 5.2.2 of IEC 62671. The use of smart devices is becoming increasingly frequent in a range of applications, from sensors and actuators to smart-type C&I embedded in equipment and in packaged systems.

334. Hitachi-GE stated earlier in GDA that smart devices will be used to perform safety functions. During GDA Steps 2 and 3, Hitachi-GE was not able to demonstrate an established process for selection and justification of smart devices to meet regulatory expectations in the UK, e.g. in relation with SAP ESS.27 (Ref. 4) and NS-TAST-GD-046 (Ref. 7).

335. I raised RO-ABWR-0030 requesting Hitachi-GE to clarify the approach for the identification of smart devices in SIS and to develop an approach for their justification. This RO also required Hitachi-GE to demonstrate the viability of the proposed justification approach through trial qualifications, for example smart devices at Class 1 and Class 2.

336. Hitachi-GE responded to RO-ABWR-0030 providing the following documents:

- ref. 67 describing the approach for smart device identification;
- ref. 68 outlining the key steps for the smart device justification in terms of PE and ICBMs; and
- ref. 69 applying the approach proposed for smart device justification in two trial examples.

337. In the early engagement on this RO resolution, Hitachi-GE clarified an intention to focus attention on the generic justification of a smart device rather than on its substantiation for a specific application. I found the approach taken in this matter proportionate for GDA because:

- the detailed arrangements for the incorporation of the smart device justification in a safety case needs to be agreed with the future licensee; and
- a database of pre-qualified smart devices has been used elsewhere in the UK nuclear industry and the approach appears to be acceptable, provided that (i) restriction of use are clearly identified in the generic justifications and (ii) the adequacy of the generic justification for the target application is carried out by competent personnel.

338. I assessed Ref. 67 and found that the approach proposed by Hitachi-GE for smart device identification (including in embedded and packaged systems) is adequate, because:

- it confirms smart devices in non-C&I systems can be identified;
- it recognises the need of C&I specialist competence (both SW and HW) when considering smart device qualification; and
- it outlines an appropriate qualification process with involvement of suitable competence in various stages of the design (from specification through detailed design to final validation).

339. I judge that in Ref. 68 Hitachi-GE shows a good appreciation of UK regulatory expectations for smart device justification, e.g.:

- For the assessment of the PE, Hitachi-GE proposes to use a tool developed by CINIF (i.e. Emphasis questionnaire, Ref. 70), which is established as relevant good practice in the UK for smart devices.

- Hitachi-GE identifies an acceptable approach for the identification of compensating measures for the gaps in the PE , based on the Cogs approach developed by CINIF (Ref. 71).
- Hitachi-GE has developed guidance on the expectations for ICBMs for different safety classes.
- The basis for the verification of the suitability of the selected ICBMs, Hitachi-GE utilises the CINIF developed strategy triangle (property-based approach, vulnerability assessment and standards compliance) based on the research project SING (Ref. 72).

340. In Ref. 69, Hitachi-GE clarified that the key information needed for the evaluation of the suitability of generic justifications for specific applications were captured through functionality and property envelopes. I find this adequate to achieve the purpose of GDA, i.e. to show that Hitachi-GE has an adequate appreciation of the expectations in the UK for smart device justification and understands that an additional step is required before the generic justification can be used in practical applications. However, I consider it is important in future stages of the project to define adequate arrangements for the verification of a generic smart device justification for a specific application in the UK ABWR C&I architecture. For this purpose, I raise an assessment finding (see point (a) of assessment finding AF-UKABWR-CI-007 below).

341. I found that the two trial justifications in Ref. 69 showed an adequate level of development for GDA. Through the use of UK contractors experienced in smart device justification, Hitachi-GE developed a good understanding of the key challenges involved in smart device justification and several lessons learned were derived from the justification examples. Ref. 69 recognises that additional analyses would be required before the two selected smart devices could be used in the UK ABWR. It is also understood that some of the lessons learned from the trial justification would require additional interaction with the smart device manufacturers. I therefore raise an assessment finding for the licensee to complete the Class 1 and Class 2 justification trials, if the devices described in Ref. 69 were to be utilised in the UK ABWR (see point (b) of assessment finding AF-UKABWR-CI-007 below).

342. Whilst Ref. 69 provides example of the justification of the higher classes (i.e. safety Class 1 and 2), it is recognised that, although graded to the safety significance, a similar approach is expected for safety Class 3 application (i.e. Emphasis for PE and ICBMs as per SAP ESS.27). I raise an assessment finding for the licensee to extend the methodology developed in Ref. 67 and Ref. 68 for safety class 3 (see point (c) of assessment finding AF-UKABWR-CI-007 below).

343. I raised RQ-ABWR-1447 (Ref. 37) to clarify some aspects related to the process developed for the smart device justification utilised for the Class 1 and Class 2 trial examples, including:

- the overall approach as an intelligent customer when using 3$^{rd}$ party contractors, in line with the expectation in NS-TAST-GD-049 (Ref. 73) and NS-TAST-GD-077 (Ref. 74);
- the key steps in the standard process expected for the smart device justification; and
- the assessor competence requirement for future smart device qualifications.

344. The answer to RQ-ABWR-1447 (Ref. 84) clarified at high level the aspects identified in this Regulatory Query. I understand that the detailed arrangements for the smart device justification will need to be agreed and further developed by the future licensee. On this basis, I find that the response to RQ-ABWR-1447 was acceptable for GDA, because it provides the basis for future smart device justifications and clearly identified the areas that will need to be further developed when specific licensee choices are considered. In this context, the response to RQ-ABWR-1447 may need to be revisited

and completed in the future by the licensee, to consider the site-specific arrangements. I therefore raise an assessment finding for the licensee to clarify in the detailed arrangements the IC and competence requirements for smart device justification (see points (d) and (e) of assessment finding AF-UKABWR-CI-007).

> *GDA Assessment Finding: **AF-UKABWR-CI-007** - During GDA, Hitachi-GE developed a methodology for smart device identification and justification, and applied it to candidate safety class 1 and safety class 2 devices. Whilst this approach was considered acceptable for GDA, this needs to be further developed to address the GDA scope limitations (for example, matters related to licensees' design choices) and some ONR assessment technical observations.*
>
> *The Licensee shall:*
>
> *a. Implement adequate arrangements to verify the suitability of generic smart device justifications for the site specific applications in the UK ABWR.*
>
> *b. Complete the safety class 1 and safety class 2 justification trials, should the smart devices considered in GDA be implemented in the UK ABWR.*
>
> *c. Extend the methodology developed for the smart device justification at safety Class 1 and safety Class 2 to safety Class 3.*
>
> *d. Complete the development of a methodology to provide adequate level of oversight and ownership of smart device justifications contracted to 3rd parties, in accordance with the site specific intelligent customer arrangements.*
>
> *e. Ensure that arrangements for the selection and evaluation of both the 3rd parties and internal assessors take into account the specialist software and hardware competencies required for smart device justification (e.g. commensurate with the safety class for the proposed application, the type and the complexity of the device).*

345. In conclusion, I consider that the approach proposed by Hitachi-GE for smart device justification is adequate for GDA.

### 4.2.7 Testing and Maintenance

346. I assessed Hitachi-GE's plans for testing and maintenance during GDA Step 4 to confirm these meet UK relevant good practice and regulatory expectations. In assessing the adequacy of risk control relating to testing and maintenance in the C&I areas, I have focussed primarily on the SSLC as this has the highest reliability requirements of any C&I system. However, I have also considered the impact of the proposals for testing and maintenance of other C&I systems.

347. RO-ABWR-0062 (Ref. 22) had been raised during GDA Step 3 because of concerns that testing and maintenance for safety systems had not been clearly communicated in the design documentation, and because UK practices for setting the frequency of tests and maintenance had not been reflected. This was a cross-cutting RO relating to the fault studies, probabilistic safety assessment, mechanical engineering and electrical engineering technical areas.

348. During GDA Step 4 Hitachi-GE submitted a document titled "Description and Substantiation of Methodology to Testing and Maintenance of Safety System" (Ref. 100). This document covers testing and maintenance requirements, testing and maintenance methodology, substantiation of testing and maintenance through a

Claims, Arguments and evidence structure, the vulnerabilities introduced by maintenance and testing, mechanical equipment associated with the SSLC, test coverage, justification of the frequency of testing, and transition from test to operational modes.

349. A graded approach to testing and maintenance is described, according to the categorisation of the safety functions being performed and the classification of the system, the design of plant equipment to ensure it is testable and maintainable, and for certain equipment to be testable and maintainable during reactor operation through system redundancy, and design to prevent single failures leading to a loss of safety function.

350. The document further describes how the testing and maintenance methodology links to the fault schedule, safety case claims, arguments, evidence (CAE) structure, and provides inputs to the PSA and testing and maintenance frequencies are derived. C&I, electrical, and mechanical items are covered by the methodology, and an example given for a specific case that describes the safety function, its categorisation and the classification of the system, the plant equipment involved in the delivery of the function, the surveillance requirements, and when testing and maintenance needs to be performed.

351. Ref. 100 describes the potential vulnerabilities introduced by testing and maintenance, including as a result of human error. The document also describes a methodology for identifying mechanical equipment delivering safety functions and the identification of the consequences of their failure, and the approach to testing using overlapping tests, and the mechanical equipment required. Justification of the frequency of tests is given, with the primary period being one month between tests. An example of transition from test to service mode is given using the High Pressure Core Flooder controlled by the SSLC.

352. Hitachi-GE provided additional GDA documentation on testing and maintenance in numerous submissions. For example, PCSR Chapter 30 “Operations” (Ref. 101), section 30.4.3 gives an overview of maintenance and inspection, and states that this will align with UK legal requirements including for risks to remain ALARP, and activities to be bounded by the Safety Case and Technical Specifications. This also describes the need to perform maintenance activities during power operation and outages, and for the design to support this. For example, this describes how plant safety is achieved through the application of Operating Technical Specifications which describe the minimum plant (e.g. system “divisions”) availability/operability and time limits on degraded plant configurations before alternative actions must be taken. It is stated that these are derived from the safety analyses in the Safety Case.

353. The maintenance philosophy for UK ABWR, (Ref. 102), states the proposed arrangements have been developed in consultation with the future licensee, and describes a number of high level objectives including maintaining the equipment reliability, early detection of hazards, compliance with the safety case and statutory and mandatory requirements, and ensuring the environmental impact has been considered. Also, Hitachi-GE states that the maintenance philosophy is intended to align with that already in force in existing UK operational reactors and developed over many years. Furthermore, Hitachi-GE states that consultation with the prospective licensee has confirmed the intention to adopt the Institute of Nuclear Power Operations (INPO) AP928 Work Management Process and also the Reliability Centred Maintenance process within the INPO AP913 Equipment Reliability Process.

354. Periodic Functional Testing is covered by the maintenance philosophy (Ref. 102) and included in the Technical Specification Surveillance Requirements to ensure that the safety criteria defined at the design stage are complied with during the operational lifetime of the plant. Hitachi-GE claim that the list of equipment subject to periodic

testing is derived primarily from the PSA model, and that this can also contribute to defining the test frequency.

355. Hitachi-GE states in the maintenance philosophy (Ref. 102) that PSA studies (Ref. 103) confirm that maintenance activities do not contribute significantly to the core damage frequency (CDF). Hitachi-GE also claim that, where reasonably practicable, the SSLC will automatically return the engineered safety feature to service should a demand arise during testing. This is confirmed in the Basis of Safety Cases on SSLC (Ref. 45). This in turn is described in the Topic Report on SSLC (Ref. 104), section 8.9.

356. The PCSR chapter 25 (Ref. 103) describes a number of purposes of probabilistic safety assessment in section 25.3.3, and this includes “f) Informing arrangements for examination, maintenance inspection and testing (e.g. the maintenance frequencies for these activities)”. Section 25.4.4.1 states that the testing and maintenance requirements have been identified using appropriate plant design information, including Piping and Instrumentation Diagram, SDD, and IBD. The effects of tests not being performed correctly are also considered. For example PCSR chapter 25 (Ref. 4) describes the identification of failure modes cause by human failure events, including those arising from testing activities. Hitachi-GE notes that detailed design information was not available during GDA and so assumptions have been made using surrogate ABWR information.

357. Because detailed design information is not available during GDA Step 4, Hitachi-GE has performed sensitivity analyses on the PSA, including testing and maintenance, to confirm that this is conservative and that there are no cliff edge effects. The PCSR analysis reported in PCSR chapter 25 also describes the consequences of assumptions on CDF. An example is given of the effect on CDF of diagnostic coverage in SSLC modules on CDF. This indicates that an undetectable fault percentage of 5% has a small effect on CDF, whilst a percentage of 20% has a large impact on CDF. However further work in the PSA and C&I areas (Refs. 103 and 80) identified that the diagnostic coverage and reliability calculations of SSLC modules for which detailed design is available have high diagnostic coverage (>80%), and coupled with higher than previously conservatively assumed hardware reliability, result in adequate control of risks.

358. I note that there is further work to be done on this in the PSA and C&I areas, but judge that a suitable methodology has been established, SSLC module reliability and diagnostic coverage appears to be acceptable, and that confidence has been provided during GDA that risks can be adequately managed.

359. The Description and Substantiation of Methodology to Testing and Maintenance of Safety System (Ref. 100) describes the methodology to testing and maintenance using a CAE approach that is based on the fault schedule and which has a graded approach based on the categorisation of safety functions and classification of systems, which encompasses all technologies and systems delivering safety functions (in PCSR chapter 5, Ref. 40), and considers the system architecture and basis for setting the frequency of testing.

360. I noted that the frequency of testing in Ref. 100 did not appear to meet UK regulatory expectations in that parts of this document stated that a monthly test is necessary with no apparent application of the methodology or justification. I therefore raised RQ-ABWR-1389 (Ref. 37), requesting Hitachi-GE to identify the factors to be considered in the identification of maintenance and test intervals. In answer to this RQ (Ref. 105), Hitachi-GE described the factors to be considered in setting the maintenance and test interval, categorised into three groups;

- group A - Equipment related (Ageing of components by test, Ageing mechanisms, Increasing maintenance requirements, input from manufacturers);

- group B -Operational and Historical (Operational needs, Operational constraints, Trend and condition monitoring data, Validity of reliability data used for PSA, Operational experience of test, Requirements to remain operational, Responding to maintenance effectiveness, planning techniques or strategies); and
- group C – Human related (Operator familiarity with plant, Workload, Extent of available automation, Human errors during or after testing, Limits of access).

361. This describes relevant factors to be considered in setting the maintenance and test interval for a range of different equipment types, including those arising from the safety case claims, and I judge this is adequate for GDA.

362. Hitachi-GE was not able to identify a document in which to place this RQ response, and so I requested that this be recorded in a suitable place during GDA. Hitachi-GE elected to place an entry into the assumption management database, with the unique reference “COM_SR.1” (Ref. 76). I confirm that this entry in the database references the response to RQ-ABWR-1389 (Ref. 105).

363. I communicated my assessment outcome to ONR inspectors in the other technical areas referenced by RO-ABWR-0062 in the form of an assessment note (Ref. 31). All accepted (Refs. 115 - 118) that the documentation presented by Hitachi-GE was adequate for the purposes of GDA and that RO-ABWR-0062 has been satisfied.

364. I performed further C&I assessment in the testing and maintenance area, considering the claims being made on platforms and on systems to provide adequate provision for testing of C&I equipment and the C&I aspects of testing of systems to ensure reliability is maintained. I identified a number of areas where information had not been provided, or where requirements had not been identified, including:

- The removal of a division of the HWBS from service to undertake repair and maintenance work requires voting arrangements to be changed temporarily. It is not clear whether a C&I interlock is planned to prevent the inadvertent removal from service of both HWBS divisions or if this is to be managed procedurally.
- It is not clear what reliability targets for the HWBS are with a divisional bypass, and if these are feasible with the system design described.
- The arrangements to support testing and maintenance and to avoid adverse interactions, such as locations, design, capability, and layout of C&I equipment, have not been completely described during GDA.

365. I consider these limitations arise because they are related to future licensee decisions regarding testing and maintenance during detailed design, such as when equipment will be available for testing and risk based operational decision making.

366. I judge these do not call into question the adequacy of the approach to testing and maintenance for the purposes of GDA, but consider these important enough to raise as an assessment finding AF-UKABWR-CI-011.

> *GDA Assessment Finding:* **AF-UKABWR-CI-011** - *In GDA, Hitachi-GE established adequate principles for the testing and maintenance of the UK ABWR C&I. As further requirements are identified post GDA, ONR’s expectation is that these principles are updated to reflect this.*
>
> *The licensee shall:*
>
> *a. Identify and address additional testing and maintenance requirements that arise as a result of detailed design;*

*b. Identify measures to prevent more than one division being removed from service (e.g. interlocking, procedural arrangements);*

*c. Address the consequences of testing and maintenance on reliability, and the measures necessary to manage risk;*

*d. Develop the approach to demonstrate that adequate coverage of all relevant components delivering a safety function is achieved to deliver the requirement of the safety case; and*

*e. Define arrangements to support testing and maintenance and to avoid adverse interactions, such as locations, design, capability, and layout of C&I equipment.*

*For further guidance see the Technical Observations for AF-UKABWR-CI-011 in Annex 5.*

### 4.2.8 Electro-Magnetic Interference

367. During GDA Step 4 I worked with the Internal Hazards inspector to assess the adequacy of the safety case relating to EMI.

368. The document "Electro Magnetic Interference Analysis Methodology" (Ref. 106) submitted during GDA Step 3 was superseded by an internal hazards submission relating to the EMI risk assessment methodology (Refs. 107, 108). My assessment of this found that the methodology for EMI risk assessment had changed and that this focussed on assessing localised EMI effects.

369. In conjunction with the Internal Hazards inspector, I raised RQ-ABWR-1315 (Ref. 37) covering the following points:

- It was not described how the requirements arising from the referenced standards would be satisfied by the methodology.
- There appeared to be gaps in the identification of EMI sources and the categorisation and classification of safety functions and systems was not complete.
- The proposed methodology did not consider that risks arising from EMI can appear some distance from the source of the EMI due to transmission along cables, through power and earthing systems, and through the air.
- All potential consequences of EMI effects did not appear to have been considered, e.g. the potential for silent failure of a system due to EMI effects.
- All significant factors in determining the EMI risk did not appear to have been considered, e.g. high switching frequencies, common power supplies, high impedance earth connections, common cable runs, etc.
- The basis of the selection of the bounding case did not appear to consider frequency/likelihood and severity of consequences arising from EMI.
- The ALARP demonstration was not clear in that it did not explicitly identify the relevant standards, did not identify how safety measures had been evaluated, did not reference a hierarchy of measures, or consider additional measures that could be applied.

370. In response to this RQ (Ref. 110), Hitachi-GE provided answers, including;

- a mapping between the original seven step process and the five step process that supersedes it and a description of which standards are applicable;

- a commitment to improve the identification of the EMI sources in an update to the submission, noting that cables can only be dealt with generically during GDA as the design has not been completed;
- further information relating to the consequences of EMI for the SRNM system;
- other significant factors will be dealt with during the detailed design phase;
- further information on the bounding case will be considered during the detailed design phase; and
- a commitment to improve the submission in relation to the selection of measures to manage EMI, with a full demonstration that EMI risk will be adequately managed during the detailed design phase.

371. I was not content with this response as I noted it still did not adequately describe how the potentially distributed nature of EMI should be considered, and how the design should avoid and account for the potential effects of mobile EMI sources such as mobile telephones and wireless communications arising from laptops and other interconnected devices that may be used during maintenance and other activities. I also noted that there were only limited improvements on how ALARP would be demonstrated post GDA.

372. As this is a technical topic associated with the C&I area, and with the agreement of the IH assessor, I discussed this further with the Hitachi-GE C&I SME in a number of Level 4 meetings (Refs. ONR-NR-CR-16-1058, ONR-NR-CR-17-29, ONR-NR-CR-17-117, ONR-NR-CR-17-173).

373. Hitachi-GE agreed to make further improvements to the document and re-submitted this (Ref. 109). My assessment of this identified improvements including a consideration of hierarchy of measures, a more detailed description of how the design principles and methodology would be applied, including the management of cable design, and including the potential presence of mobile EMI emitters. I also noted that the submission has improved references to appropriate C&I documents, and has improved the description of the ALARP process that will be applied post-GDA.

374. I judge this to be adequate for the purposes of GDA in that the EMI TR now acknowledges the potentially distributed nature of EMI, identifies an adequate methodology for the management of risk arising from EMI, and provides an improved framework for ALARP demonstration. My expectation is that post-GDA the licensee will apply the EMI methodology and provide an ALARP demonstration that the risks arising from EMI are being adequately managed.

### 4.2.9 Cyber security

375. This assessment is documented in Annex 6 of this report.

## 4.3 Regulatory Issues

376. Regulatory Issues (RIs) are matters that ONR judge to represent a ’significant safety shortfall’ in the safety case or design and are the most serious regulatory concerns. RIs are required to be addressed before a DAC can be issued.

377. No RIs were identified in C&I area in the close-out of the UK ABWR GDA.

## 4.4 Regulatory Observations

378. A Regulatory Observation (RO) is raised when ONR identifies a potential regulatory shortfall which requires action and new work by Hitachi-GE for it to be resolved. Each RO can have several associated actions.

379. A summary of ROs related to Control and Instrumentation can be found in Annex 4

380. During the Step 3 assessment a number of regulatory concerns were raised which were linked to the findings of the Step 2 C & I Assessment (Ref. Step 2 assessment). To ensure these matters were adequately addressed a series of Regulatory Observations were issued which clearly set out the regulatory concern and regulatory expectations. Table 5 below identifies the RO, the link to the assessment scope and the status.

| Regulatory Observation Title and Number | Regulatory Observation Title |
|---|---|
| RO-ABWR-0026 | Back-up Building C & I |
| RO-ABWR-0027 | Hardwired Back-up system |
| RO-ABWR-0028 | Safety System Logic & Control (SSLC) Class 1 HMI |
| RO-ABWR-0029 | SSLC Production Excellence |
| RO-ABWR-0030 | Embedded C & I subsystems and smart systems |
| RO-ABWR-0031 | SSLC & Support System Architecture |
| RO-ABWR-0032 | SSLC Design |
| RO-ABWR-0061 | Reactor Pressure Vessel Instrumentation Connections |
| RO-ABWR-0062 | Testing and Maintenance of Safety Systems |

**Table 5.** Summary of UK ABWR C&I Regulatory Observations.

381. Hitachi-GE developed resolution plans, as listed in Annex 4, to identify activities and submissions to complete the actions identified in each RO. I have documented my assessment of these, as necessary, in the relevant sections of my report, and have closed each of these during GDA Step 4. I have recorded unresolved points that are not normal regulatory business, as necessary, in assessment findings listed in Annex 5 of this report.

### 4.5 Comparison with standards, guidance and relevant good practice

382. In my assessment, I sought confirmation that the C&I design proposed in GDA for the UK ABWR adequately considers relevant international standards and relevant good practice applicable in the UK.

383. With regard to ONR SAPs (Ref. 4), I assessed the C&I submissions from Hitachi-GE (including the PCSR Chapter 14 in Ref. 39 and the BSCs in Refs. 44-55) against the relevant SAPs. I also reviewed the result of the SAP compliance exercise by Hitachi-GE in Ref. 57. I am therefore content that the proposed C&I design aligns with UK regulatory expectations. More information on my assessment and the conclusions are presented as part of Section 4.2.1 of this report. My expectation is that the detailed design information will confirm this conclusion, providing evidence that the principles established in GDA are suitably applied in future stages of the project.

384. In Step 3, I raised RQ-ABWR-0490 (Ref. 37), for Hitachi-GE to identify the key standards considered in the design of UK ABWR C&I. In Step 4, Hitachi-GE provided a revised version of the RQ response (Ref. 77), which I found adequate for GDA, because it identifies the key standards to develop the C&I design expected in GDA for the UK ABWR. Ref. 77 also provides a mapping between the IEC standards expected in the UK and Japanese standards, used for the original design of certain C&I systems which are common to the reference design. I found this a suitable approach to inform the review of these systems and to help identifying any gap.

385. Within GDA Hitachi-GE provided compliance documents against the key standards (e.g. IEC 62566 for the Class 1 platform, Ref. 56) and the most relevant clauses of

other standards were covered as part of the BSCs and lower tier documents (e.g. Refs. 44 and 58 for the compliance against IEC 61513 for the SSLC). As discussed in Section 4.2.1, the complete demonstration of the compliance with all of the standards identified in Ref. 77 will need to consider detailed design information (see assessment finding AF-UKABWR-CI-001 in Annex 5).

386. In assessing whether the UK ABWR meets relevant good practice in the UK, I focussed on established nuclear facilities and new build projects proposed for the UK. I am satisfied that the UK ABWR C&I design aligns with modern nuclear design principles and that it meets UK regulatory expectations.

### 4.6 Overseas regulatory interface

387. ONR has formal information exchange agreements with a number of international nuclear safety regulators, and collaborates through the work of the International Atomic Energy Agency (IAEA) and the Organisation for Economic Co-operation and Development Nuclear Energy Agency (OECD-NEA). This enables ONR to benefit from overseas regulatory assessments of reactor technologies, where they are relevant to the UK. It also enables the sharing of regulatory assessment findings, which can expedite assessment and helps promote consistency.

388. ONR also represents the UK on the Multinational Design Evaluation Programme (MDEP).This seeks to:

- enhance multilateral co-operation within existing regulatory frameworks; and
- encourage multinational convergence of codes, standards and safety goals in order to facilitate the licensing of new reactors, including those being developed by Gen IV international Forum.

389. During this assessment I chaired the ABWR Technical Expert Sub Group (TESG) on C&I. This considered international experience of the ABWR and similar reactors and received input from the nuclear regulators from Japan, Sweden, the USA, and the UK. Topics discussed relevant to my assessment included:

- the relevance of differences in the C&I regulations in different countries;
- C&I architecture and interconnection between systems;
- different approaches to the assessment of C&I systems used on the ABWR reactor;
- ABWR Reactor Vessel Instrumentation design and lessons learned; and
- use of Field Programmable Gate Array technology in C&I safety systems.

390. I have also participated in a number of meetings of the MDEP Digital I&C Working Group (DICWG), and contributed to the development of Common Positions (CP) in conjunction with a wider group of international regulators, including China, Finland, France, India, Japan, Russia, South Korea, South Africa, Sweden, and USA.

391. I have reviewed the UK ABWR C&I designs against each of the CP's and have confirmed that these are broadly in agreement with the principles identified in these.

392. I have also had bi-lateral meetings with the regulators from France, Japan, and the USA to discuss specific technical aspects of C&I.

### 4.7 GDA Issues

393. I did not identify any GDA Issues during my assessment of the UK ABWR C&I. I have identified a number of findings which I do not consider are of sufficient importance to

prevent the issue of a Design Acceptance Confirmation (DAC), but which I consider are important enough to raise as assessment findings. These are discussed below.

### 4.8 Assessment findings

394. In some areas my assessment during GDA Step 4 has identified limitations in the safety case, due to lack of detailed information, conflicting information, in a few cases where the principles established do not appear to have been fully reflected in the design presented, and for other reasons. As a result I will need safety case improvements to underpin my conclusions, and these are identified as Assessment Findings. I have raised Assessment Findings to cover items such as safety case clarity, standards' compliance demonstration, and implementation of process improvements.

395. During my assessment 19 residual matters were identified for a future licensee to take forward in their site-specific safety submissions. Details of these are contained in Annex 5 of this report, providing reference to the section of this report which clarifies the context of the AF and, where necessary, a link to relevant technical observations raised in the detailed review of the submissions (Refs. 32-36). I note that TO2s represent examples of observations arising from the Hitachi-GE submissions identified in a review performed on sampling basis and, for this reason, should be addressed considering the wider implications on the overall safety case.

396. These matters do not undermine the conclusions arising from my assessment and are primarily concerned with the provision of site specific safety case evidence, which will usually become available as the project progresses through the detailed design, construction and commissioning stages. These items are captured as assessment findings.

397. I have recorded residual matters as assessment findings if one or more of the following apply:

- site specific information is required to resolve this matter;
- resolving this matter depends on licensee design choices;
- the matter raised is related to operator specific features / aspects / choices;
- the resolution of this matter requires licensee choices on organisational matters;
- to resolve this matter the level of detail of the design needs to be beyond what can reasonably be expected in GDA (e.g. manufacturer/supplier input is required; or areas where the technology changes quickly, and so to avoid obsolescence of design); and
- to resolve this matter the plant needs to be at some stage of construction / commissioning.

398. Assessment Findings are residual matters that must be addressed by the Licensee and the progress of this will be monitored by the regulator.

# 5 CONCLUSIONS

1. This report presents the findings of my Step 4 Control and Instrumentation assessment of the Hitachi-GE UK ABWR against relevant SAPs, TAGs, and relevant good practice, as described in the report, and recorded in Annex 1, Annex 2, and Annex 3.

2. To conclude, I am broadly satisfied with the claims, arguments and evidence laid down within the PCSR and supporting documentation for C&I. I consider that, from a C&I view point, the Hitachi-GE UK ABWR design is suitable for construction in the UK subject to future permissions and permits beings secured. However, this conclusion is subject to assessment of additional information that becomes available as the GDA Design Reference is supplemented with additional details.

3. Whilst no GDA Issues were identified in the close-out of UK ABWR GDA Step 4, a number of assessment findings (Annex 5) were identified. These are for future licensee to address and take forward in their site-specific safety submissions. These matters do not undermine the generic safety submission and require licensee input/decision.

## 5.1 Key Findings from the Step 4 Assessment

The key findings of my Step 4 assessment are that

- The PCSR and supporting documentation submitted by Hitachi-GE in GDA Step 4 adequately identify and justify the main C&I safety-important systems expected in a modern nuclear reactor.
- The principal design and implementation standards used by Hitachi-GE for all C&I safety-important systems are broadly in accordance with those expected in the nuclear sector in the UK.
- The C&I safety case for the sampled key C&I systems and platforms is broadly in line with ONR's expectations.
- The cyber security principles expected to be considered as part of the justification of the C&I for a modern nuclear power plant have been established.
- Hitachi-GE has adequately addressed the C&I Regulatory Observations raised by ONR in previous GDA steps.
- The safety case submitted by Hitachi-GE achieves the purpose of GDA, i.e. to de-risk future activities in the development of the UK ABWR C&I detailed design.

My judgement is based upon the following factors:

- review of the C&I architecture proposed for the UK ABWR;
- assessment of the key submissions, including the PCSR Chapter 14 and the Basis of Safety Cases for the overall UK ABWR C&I architecture and key safety systems;
- sampling of the key supporting documents, providing the evidence to support claims and arguments identified in the C&I safety case; and
- discussions with other relevant disciplines (including Fault Studies, Probabilistic Safety Assessment, Human Factors and Internal Hazards) regarding the overall claims on the UK ABWR C&I systems.

In my assessment I have not identified significant technical concerns that require GDA Issues to be raised. However, I made a number of observations during my assessment of the GDA submissions. Because these matters do not undermine the generic safety submission but require licensee input/decision at a specific site, these are for a future licensee to consider and take forward in their site-specific safety submissions. These C&I assessment findings cover the following areas:

- the justification of the FPGA used for the Class 1 SSLC system as the detailed design develops (e.g. independent verification at the board level, verification of the FPGA configuration, verification of macros, tools, maintenance terminal);
- considerations in the C&I detailed design development of key activities and analyses, to confirm the principles justified in GDA (e.g. regarding diversity and standards compliance);
- development of adequate intelligent customer arrangements covering key areas of interest for ONR (e.g. ownership of the safety case, smart device justifications and surveillance of 3rd party activities);
- consistency between claims in Fault Studies and Probabilistic Safety Assessment and the engineering substantiation in C&I (e.g. regarding reliability or resilience of the plant control system to common mode failure);
- testing and maintenance, to account for the detailed design information;
- considerations in the development of the HMI in areas of particular interest such as transfer switches and alarms; and
- consideration of a number of technical observations out of scope for GDA, but considered important in licensing, to ensure the clarity and consistency of the safety case.

Overall, based on the samples undertaken, I am satisfied that the claims, arguments and evidence laid out within the PCSR and supporting documentation submitted as part of the GDA process present an adequate safety case for the generic UK ABWR design in the area of C&I. For this reason, the UK ABWR should be awarded a DAC.

I consider that from a C&I perspective, the UK ABWR design is suitable for construction in the UK, subject to further detailed design that meets regulatory expectations, and to completion of future permissions and permits beings secured.

# 6 REFERENCES

1. ONR, Generic Design Assessment (GDA) of new nuclear power stations, ONR website: www.onr.org.uk/new-reactors/index.htm.
2. ONR, Summary report of the Step 3 Generic Design Assessment (GDA) of Hitachi-GE Nuclear Energy's UK Advanced Boiling Water Reactor (UK ABWR), ONR website: http://www.onr.org.uk/new-reactors/uk-abwr/reports/step3/uk-abwr-step-3-summary-report.pdf.
3. ONR, Guidance on Mechanics of Assessment, TRIM 2013/204124.
4. ONR, Safety Assessment Principles for Nuclear Facilities, November 2014, ONR website: www.onr.org.uk/saps/saps2014.pdf.
5. ONR, NS-TAST-GD-003 Rev. 7, Safety Systems, ONR website: http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-003.pdf.
6. ONR, NS-TAST-GD-005 Rev. 7, Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable), ONR website: http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-005.pdf.
7. ONR, NS-TAST-GD-046, Rev. 3, Computer Based Safety Systems, ONR website: www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-046.pdf.
8. ONR, NS-TAST-GD-051 Rev. 4, The purpose, scope, and content of safety cases, ONR website: http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-051.pdf.
9. ONR, NS-TAST-GD-094, Rev. 0, Categorisation of Safety Functions and Classification of Structures and Components, ONR website: http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-094.pdf.
10. ONR, New nuclear reactors: Generic Design Assessment Guidance to Requesting Parties, ONR-GDA-GD-001 Revision 3, ONR website: http://www.onr.org.uk/new-reactors/ngn03.pdf.
11. ONR, NS-PER-GD-014, Purpose and Scope of Permissioning, ONR website: www.onr.org.uk/operational/assessment/ns-per-gd-014.pdf.
12. ONR, ONR-GDA-AP-15-02 Revision 1, ONR Step 4 Assessment Plan – control and instrumentation, TRIM 2016/406036.
13. ONR, ONR-GDA-AR-15-006 Revision 0, GDA Step 3 Assessment of the Control and Instrumentation of Hitachi GE's UK Advanced Boiling Water Reactor (UK ABWR), TRIM 2015/224084.
14. ONR, RO-ABWR-0026, Back-up Building Control and Instrumentation, TRIM 2015/15966.
15. ONR, RO-ABWR-0027, Hardwired Back-up System, TRIM 2015/15970.
16. ONR, RO-ABWR-0028, Safety System Logic & Control (SSLC) Class 1 HMI, TRIM 2015/15974.
17. ONR, RO-ABWR-0029, SSLC Production Excellence, TRIM 2015/15979.
18. ONR, RO-ABWR-0030, Embedded C&I subsystems and smart devices, TRIM 2015/15983.
19. ONR, RO-ABWR-0031, SSLC and Support System Architecture, TRIM 2015/15987.
20. ONR, RO-ABWR-0032, Safety System Logic Control (SSLC) Design, TRIM 2015/15992.
21. ONR, RO-ABWR-0061, Reactor Pressure Vessel Instrumentation Connections, TRIM 2015/357979.
22. ONR, RO-ABWR-0062, Testing and Maintenance of Safety Systems, TRIM 2015/357997.
23. ONR, RO-ABWR-0026 close-out assessment, TRIM 2016/197068.
24. ONR, RO-ABWR-0027 close-out assessment, TRIM 2017/143434.
25. ONR, RO-ABWR-0028 close-out assessment, TRIM 2017/288302.
26. ONR, RO-ABWR-0029 close-out assessment, TRIM 2017/172195.
27. ONR, RO-ABWR-0030 close-out assessment, TRIM 2017/259408.
28. ONR, RO-ABWR-0031 close-out assessment, TRIM 2017/188777.
29. ONR, RO-ABWR-0032 close-out assessment, TRIM 2017/290453.
30. ONR, RO-ABWR-0061 close-out assessment, TRIM 2017/236041.

31. ONR, RO-ABWR-0062 close-out assessment, TRIM 2017/327078.
32. Altran, S.P1715.41.01 Issue 2.0, Structure and clarity of the C&I safety case, Review Area 1, UK ABWR, TRIM 2017/441488.
33. Altran, S.P1715.41.02 Issue 2.0, Evidence of adequacy of C&I architecture, Review Area 2, UK ABWR, TRIM 2017/441499.
34. Altran, S.P1715.41.03 Issue 2.0, Confirmation of the adequacy of the platforms, Review Area 3, UK ABWR, TRIM 2017/441513.
35. Altran, S.P1715.41.04 Issue 2.0, Confirmation of the adequacy of the systems, Review Area 4, UK ABWR, TRIM 2017/442756.
36. Altran, S.P1715.41.05 Issue 2.0, Adequacy of the Human Machine Interfaces, Review Area 5, UK ABWR, TRIM 2017/441535.
37. ONR, UK ABWR Final RQ Tracker – December 2017, TRIM 2017/339475.
38. Hitachi-GE, UK ABWR - GA10-0511-0006-00001 - XD-GD-0036 - Rev 3 - GDA Safety Case Development Manual.
39. Hitachi-GE, UK ABWR - GA91-9101-0101-14000 - 3E-GD-A0063 – Rev C - Generic PCSR Chapter 14: Control and Instrumentation.
40. Hitachi-GE, UK ABWR - GA91-9101-0101-05000 - XE-GD-0645 – Rev C - Generic PCSR Chapter 5 - Generic Design Aspects.
41. UK ABWR - GA91-9101-0101-21000 - 3E-GD-A0060 – Rev C - Generic PCSR Chapter 21: Human Machine Interface.
42. Hitachi-GE, UK ABWR - GA91-9201-0001-00022 - UE-GD-0071 - Rev 6 - Topic Report on Fault Assessment.
43. Hitachi-GE, UK ABWR - GA91-9201-0001-00082 - AE-GD-0229 - Rev 2 - Topic Report on Fault Assessment for SFP and Fuel Route.
44. Hitachi-GE, UK ABWR, GA91-9201-0002-00022 - 3D-GD-A0001 - Rev. 4 - Basis of Safety Cases on Control and Instrumentation Architecture.
45. Hitachi-GE, UK ABWR, GA91-9201-0002-00073 - 3D-GD-A0008 - Rev. 4 - Basis of Safety Cases on Safety System Logic and Control System.
46. Hitachi-GE, UK ABWR, GA91-9201-0002-00111 - 3D-GD-A0016 - Rev. 3 - Basis of Safety Cases on Safety Auxiliary Control System.
47. Hitachi-GE, UK ABWR, GA91-9201-0002-00029 - 3D-GD-A0009 - Rev. 2, Basis of Safety Cases on Hardwired Backup System.
48. Hitachi-GE, UK ABWR, GA91-9201-0002-00110 - 3D-GD-A0015 - Rev. 3 - Basis of Safety Cases on Severe Accident C&I System.
49. Hitachi-GE, UK ABWR, GA91-9201-0002-00070 - 3D-GD-D010 - Rev. 4 - Basis of Safety Cases on Plant Control System.
50. Hitachi-GE, UK ABWR, GA91-9201-0002-00071 - 3D-GD-A0010 - Rev. 3 - Basis of Safety Cases on Reactor / Turbine Auxiliary Control System.
51. Hitachi-GE, UK ABWR, GA91-9201-0002-00072 - 3D-GD-A0011 - Rev. 3 - Basis of Safety Cases on Plant Computer System.
52. Hitachi-GE, UK ABWR, GA91-9201-0002-00109 - 3E-GD-A0166 - Rev.1 - Basis of Safety Cases on Overall Human-machine Interface.
53. Hitachi-GE, UK ABWR, GA91-9201-0002-00060 - 3E-GD-A0029 - Rev.2 - Basis of Safety Cases on Main Control Room Human-machine Interface.
54. Hitachi-GE, UK ABWR, GA91-9201-0002-00061 - 3E-GD-A0030 - Rev.2 - Basis of Safety Cases on Remote Shutdown System Human-machine Interface.
55. Hitachi-GE, UK ABWR, GA91-9201-0002-00062 - 3E-GD-A0031 - Rev.2 - Basis of Safety Cases on Backup Building Human-machine Interface.
56. Hitachi-GE, UK ABWR - GA91-9920-0003-00001 - 3E-GD-A0134 - Rev 10 - Safety Plan for NCFS-1.
57. Hitachi-GE, UK ABWR - GA91-9201-0001-00048 - 3E-GD-A0074 - Rev 2 - Topic Report on SAP Compliance on Control and Instrumentation.
58. Hitachi-GE, UK ABWR - GA91-9201-0003-02194 - 3E-GD-A0491 - Rev 0 - IEC 61513 Compliance Report for SSLC.
59. Hitachi-GE, UK ABWR - GA91-9201-0003-02193 - 3E-GD-A0490 - Rev 0 - NSEDP and SPC Sources and Completeness (Response to RQ-ABWR-1439).

60. Hitachi-GE, Full response to RQ-ABWR-1422 - Rev 1 - Clarification Regarding PCSR C&I Chapter 14 Rev. C (Draft 11).
61. ONR, ONR-NR-AR-17-016 - Step 4 Assessment of Fault Studies for the UK ABWR, TRIM 2017/98169.
62. Hitachi-GE, UK ABWR - GA91-9201-0003-00148 - AE-GD-0184 - Rev 6 - Initiating Event Analysis for Internal Event at Power Level 1 PSA.
63. Hitachi-GE, UK ABWR - GA91-9201-0003-01513 - 3E-GD-D147 - Rev 1 - The Notification to ONR of the Correction of the Safety Class of UK ABWR PCntIS from B-2 to B-3.
64. Hitachi-GE, UK ABWR - GA91-9201-0003-01584 - 3E-GD-D157 - Rev 1 - Response to Queries Claims on Plant Control System - Change of Safety Class from B2 to B3 (Response to RQ-ABWR-1011).
65. Hitachi-GE, UK ABWR - GA91-9201-0003-02177 - 3E-GD-D200 - Rev 1 - Clarification regarding the safety classification of the UK ABWR plant control system (response to RQ-ABWR-1434).
66. Hitachi-GE, UK ABWR - GA91-9201-0003-00814 - AE-GD-0472 - Rev 1 - ALARP Assessment Report for Fuel Route.
67. Hitachi-GE, UK ABWR - GA91-9201-0003-00700 - 3E-GD-A0175 - Rev 1 - Design Procedure for Embedded C&I.
68. Hitachi-GE, UK ABWR - GA91-9201-0003-00844 - 3E-GD-A0217 - Rev 0 - General approach to the justification of SMART Devices.
69. Hitachi-GE, UK ABWR - GA91-9201-0001-00046 - 3E-GD-A0177 - Rev 3 - Topic Report on SMART Devices.
70. Evaluation of Mission Imperative High-integrity Applications of Smart Instruments for Safety – tool and questionnaire version v2.4.1. Retrieved from CINIF.
71. D/632/4381/1 v1.0, Cogs8 Project Report: Part 1 – Smart instruments, Adelard LLP, 2011. Retrieved from CINIF.
72. P Bishop, N Chozos, D Sheridan, T King and A Jones. Guide to software analysis techniques.
73. NS-TAST-GD-049, Revision 5, Licensee Core and Intelligent Customer Capabilities, April 2016. www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-049.pdf.
74. NS-TAST-GD-077, Revision 3, Supply Chain Management Arrangements for the Procurement of Nuclear Safety Related Items or Services, February 2015. www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-077.pdf.
75. UK ABWR - GA91-9101-0101-27000 - HFE-GD-0057 - Rev C - Generic PCSR Chapter 27: Human Factors.
76. Hitachi-GE - UK ABWR - GA91-9201-0003-02055 - XD-GD-0049 - Rev 1 - Comprehensive List in GDA for Requirements & Assumptions to be Transferred to Operating Regime.
77. Hitachi-GE - UK ABWR - GA91-9201-0003-00925 - 3E-GD-A0183 - Rev 1 - C& I Review of Standards, Codes and Guides (Response to RQ-ABWR-0490).
78. Hitachi-GE - UK ABWR - GA91-9101-0301-00001 - XE-GD-0239 – Draft D - CSA Appendix C.2 Cyber Design Basis Threat.
79. Hitachi-GE - UK ABWR - GA91-9101-0301-00001 - XE-GD-0239 – Rev. 0 - CSA Appendix C.2 Cyber Design Basis Threat.
80. Hitachi-GE - UK ABWR - GA91-9201-0001-00045 - 3E-GD-A0058 - Rev 2 - Topic Report on Class 1 Platform.
81. ONR, ONR-NR-AR-17-014 - Step 4 Assessment of PSA for the UK ABWR, TRIM 2017/98147.
82. Hitachi-GE, UK ABWR - GA91-9201-0003-01904 - UE-GD-0660 - Rev 1 - Study on All Rod Insertion Fault.
83. Licensing of safety critical software for nuclear reactors. Common position of international nuclear regulators and authorised technical support organisations. Revision 2015, www.onr.org.uk/software.pdf.
84. Hitachi-GE, UK ABWR - GA91-9201-0003-02281 3E-GD-A0502 - Rev 0 - Clarification Regarding the Smart Device Justification Process (Response to RQ-ABWR-1447).

85. Hitachi-GE, UK ABWR - GA91-9201-0003-00662 - Rev0 - 3E-GD-A0173 - Proposed Detail Project-Schedule for New Class 1 Platform.
86. Hitachi-GE, UK ABWR - GA91-9201-0002-00090 - 3E-GD-A0171 - Rev 5 - Safety Concept for vCOSS/NCFS-1 Platform.
87. Hitachi-GE, UK ABWR - GA32-9920-0010-00001 - 3E-GD-A0095 - Rev 3 - Evaluation of Design Tools.
88. Hitachi-GE, UK ABWR - GA91-9201-0001-00051 - 3E-GD-A0169 - Rev 3 - Topic Report on ICBM for FPGA.
89. Hitachi-GE, UK ABWR - GA91-9201-0003-02175 - 3E-GD-A0481 - Rev 0 - Hardwired Backup System Technology (Response to RQ-ABWR-1430).
90. Hitachi-GE, UK ABWR - GA91-9201-0001-00058 - 3E-GD-A0105 - Rev 2 - Topic Report on Hardwired Backup System.
91. Hitachi-GE, UK ABWR - GA91-9201-0001-00153 - 3E-GD-A0364 - Rev 1 - Topic Report on Hardwired Backup System Platform.
92. Hitachi-GE, UK ABWR - GA91-9201-0001-00044 - 3E-GD-A0059 - Rev 1 - Topic Report on Class 3 Platform.
93. Hitachi-GE, UK ABWR - GA91-9201-0003-00663 - 3E-GD-A0174 - Rev 3 - Design of the SSLC HMI and the Selected Technology.
94. Hitachi-GE, UK ABWR - GA91-9201-0003-00577 - 3E-GD-A0154 - Rev 1 - Functionality of Class 1 HMI for the SSLC.
95. Hitachi-GE, UK ABWR - GA91-9201-0003-01919 - HFE-GD-0474 - Rev A - UK ABWR Alarm Processing and Presentation Strategy.
96. Hitachi-GE, UK ABWR - GA91-9201-0003-01936 - 3E-GD-A0137 - Rev 0 - Alarm Basic Design Specification.
97. Hitachi-GE, UK ABWR - GA91-9201-0003-00427 - BKE-GD-0020 - Rev 2 - Room Data Sheets for Internal Hazards Assessment.
98. Hitachi-GE, UK ABWR - GA91-9201-0003-01423 - AE-GD-0740 - Rev 2 - Task Report 3/9 for Fire PSA (Cable Selection and Detailed Circuit Analysis).
99. Hitachi-GE, UK ABWR - GA91-9201-0003-01749 - AE-GD-0832 - Rev 0 - Multiple Spurious Operation (MSO) Scenario Identification Report.
100. Hitachi-GE, UK ABWR - GA91-9201-0003-01099 - 3E-GD-A0278 - Rev 0 - Description and Substantiation of Methodology to Testing and Maintenance of Safety System.
101. Hitachi-GE, UK ABWR - GA91-9101-0101-30000 - QGI-GD-0012 - Rev C - Generic PCSR Chapter 30: Operation.
102. Hitachi-GE, UK ABWR - GA91-9201-0003-01498 - XE-GD-0613 - Rev A - UK ABWR GDA Maintenance Philosophy.
103. Hitachi-GE, UK ABWR - GA91-9101-0101-25000 - AE-GD-0171 - Rev C - Generic PCSR Chapter 25: Probabilistic Safety Analysis.
104. Hitachi-GE, UK ABWR - GA91-9201-0001-00052 - 3E-GD-A0104 - Rev 3 - Topic Report on Safety System Logic and Control System.
105. Hitachi-GE, UK ABWR - GA91-9201-0003-02098 - 3E-GD-A0476 - Rev 0 - Testing and Maintenance Frequencies (Response to RQ-ABWR-1389).
106. Hitachi-GE, UK ABWR - GA91-9201-0003-00198 - 3E-GD-A0084 - Rev 1 - Electro Magnetic Interference Analysis Methodology.
107. Hitachi-GE - UK ABWR - GA91-9201-0001-00083 - 3E-GD-A0096 - Rev 2 - Topic Report of Electro Magnetic Interference.
108. Hitachi-GE - UK ABWR - GA91-9201-0001-00083 - 3E-GD-A0096 - Rev 3 - Topic Report of Electro Magnetic Interference.
109. Hitachi-GE - UK ABWR - GA91-9201-0001-00083 - 3E-GD-A0096 - Rev 4 - Topic Report of Electro Magnetic Interference.
110. Hitachi-GE, UK ABWR - GA91-9201-0003-02023 - 3E-GD-A0461 - Rev 0 - ONR Queries on the Assessment of Electro Magnetic Interference (EMI) Hazards (Response to RQ-ABWR-1315).
111. Hitachi-GE, UK ABWR - GA91-9201-0003-01676 - 3E-GD-A0407 - Rev 0 - SSLC Design and Development Life Cycle Plan (Response to RQ-ABWR-1035).
112. Hitachi-GE, UK ABWR - Excess Flow Check Valve Specification.

113. Hitachi-GE, UK ABWR - GA91-9201-0003-02251 - 3E-GD-A0494 - Rev 1 - Clarification of Transfer Switches Design for UK ABWR (Response to RQ-ABWR-1470).
114. ONR, UK ABWR - GDA - C&I - List of prospective AFs and validation, TRIM 2017/157521.
115. ONR, Fault studies acceptance of closure of RO-ABWR-0062 Testing and Maintenance, TRIM 2017/326867.
116. ONR, PSA acceptance of closure of RO-ABWR-0062 Testing and Maintenance, TRIM 2017/326871.
117. ONR, Electrical acceptance of closure of RO-ABWR-0062 Testing and Maintenance, TRIM 2017/326876.
118. ONR, Mechanical acceptance of closure of RO-ABWR-0062 Testing and Maintenance, TRIM 2017/326878.
119. Hitachi-GE, UK ABWR, GA91-9201-0001-00040 - HFE-GD-0063 - Rev E - Allocation of Function Report.
120. Hitachi-GE, UK ABWR - GA91-9201-0001-00190 - 3E-GD-D122 - Rev 2 - Topic Report on Plant Control System.
121. Spare.
122. Hitachi-GE, UK ABWR - GA91-9201-0001-00147 - 3E-GD-A0290 - Rev 2 - Topic Report on Severe Accident C&I System.
123. Hitachi-GE, UK ABWR - GA91-9201-0003-00987 - 3E-GD-A0186 - Rev 0 - Diveristy in detection of fault sequences.
124. Hitachi-GE, UK ABWR - GB21-2109-0001-00001 - 310PB17-771 - Rev 2 - Reactor Pressure Vessel Instrument System System Diagram.
125. Hitachi-GE, UK ABWR - GA91-9201-0001-00056 - 3E-GD-A0129 - Rev 2 - Topic Report on Reactor Pressure Vessel Instrument System.
126. Hitachi-GE, UK ABWR - GA91-9201-0002-00041 - HPE-GD-H006 - Rev 4 - Basis of Safety Cases on Heating Ventilating and Air Conditioning System.
127. Hitachi-GE, UK ABWR - GA91-9201-0001-00148 - 3E-GD-A0289 - Rev 1 - Topic Report on Safety Auxiliary Control System.
128. Hitachi-GE, UK ABWR - GA91-9201-0003-02102 - 3E-GD-A0477 - Rev 0 - Independence of Hardwired Backup System Divisions (Response to RQ-ABWR-1391).
129. Hitachi-GE, UK ABWR - GA91-9201-0001-00149 - 3E-GD-A0298 - Rev 1 - Topic Report on Reactor / Turbine Auxiliary Control System.
130. Fukushima Report - WS6 - Final Report - ONR-FR-REP-11-002 Revision 1.
131. Hitachi-GE, UK ABWR - GA91-9201-0003-00619 - AE-GD-0363 - Rev 0 - Accident Management Guideline (After Core Damaged) for UK ABWR.
132. TSC250_040_002 Review of Primary Protection System Design and Development Process (RO-ABWR-32) Final v2_0.
133. TSC250_040_003 Review of Primary Protection System Design Methodology (RO-ABWR-029) Final v2.0.
134. Multinational Design Evaluation Programme (MDEP), Common Position CP-DICWG-13, Common position on spurious actuation, 2017.
135. Hitachi-GE, UK ABWR - GA91-9201-0003-00886 - 3E-GD-A0435 - Rev 1 - Formal Verification Result.
136. ONR, Reactor Building Crane and Spent Fuel Export Assessment Note, TRIM 2017/172185.
137. Spare.
138. ONR, UK ABWR Additional Protection against Control Rod Movement Faults (RO-ABWR-0077) – Determination of unmitigated consequences - File Note, TRIM 2017/196819.
139. Hitachi-GE, UK ABWR - GA91-9201-0003-00808 - 3E-GD-A0212 - Rev 0 - Measures against Common Cause Failure of Reactor Vessel Instrumentation sensing line.
140. Hitachi-GE UK ABWR - GA91-9201-0003-01786 - AE-GD-0850 - Rev 1 - Risk Insights on Reactor Vessel Instrumentation (Response to RQ-ABWR-1134).

141. Hitachi-GE UK ABWR - GA31-1101-0001-00001 - ZE-GD-0004 - Rev 1 - Investigation of Pipe Whipping Effects Associated with the Postulated Rupture of Piping.
142. Hitachi-GE UK ABWR - GA91-9201-0001-00131 - SE-GD-0268 - Rev 3 - Topic Report on Internal Hazards Inside PCV.
143. Hitachi-GE UK ABWR - GA91-9201-0003-01873 - OZD-GD-0001 - Rev 2 - Pipe Whip and Impact Evaluation Evidence Document.
144. Hitachi-GE UK ABWR - GA91-9201-0004-00025 - 3E-GD-A0087 - Rev 0 - Resolution Plan for RO-ABWR-0026 Back-up Building C&I.
145. Hitachi-GE UK ABWR - GA91-9201-0005-00025 - 3E-GD-A0108 - Rev 0 - Detailed Gantt Chart for UK ABWR Resolution Plan (Corresponding to RO-ABWR-0026) - 23 December 2014.
146. Hitachi-GE UK ABWR - GA91-9201-0004-00026 - 3E-GD-A0090 - Rev 5 - Resolution Plan for RO-ABWR-0027 - Hardwired Back Up System.
147. Hitachi-GE UK ABWR - GA91-9201-0005-00026 - 3E-GD-A0109 - Rev 4 - Detailed Gantt Chart for UK ABWR Resolution Plan (Corresponding to RO-ABWR-0027).
148. Hitachi-GE UK ABWR - GA91-9201-0004-00027 - 3E-GD-A0091 - Rev 0 - Resolution Plan for RO-ABWR-0028 Safety System Logic & Control (SSLC) Class 1 HMI.
149. Hitachi-GE UK ABWR - GA91-9201-0005-0027 - 3E-GD-A01100 - Detailed Gantt Chart for UK ABWR Resolution Plan (Corresponding to RO-ABWR-0028).
150. Hitachi-GE UK ABWR - GA91-9201-0004-00028 - 3E-GD-A0089 - Rev 1 - Resolution Plan for RO-ABWR-0029 - SSLC Production Excellence.
151. Hitachi-GE UK ABWR - GA91-9201-0005-00028 3E-GD-A0111 - Rev 1 - Detailed Ghant [sic] Chart for UK ABWR Resolution Plan - Corresponding to RO-ABWR-0029.
152. Hitachi-GE UK ABWR - GA91-9201-0004-0029 - Rev 0 - Resolution Plan for RO-ABWR-0030 Embedded C & I Subsystems and Smart Devices.
153. Hitachi-GE UK ABWR - GA91-9201-0005-0029 - Rev 0 - 3E-GD-A0112 - Detailed Gantt Chart for UK ABWR Resolution Plan (Corresponding to RO-ABWR-0030).
154. Hitachi-GE UK ABWR - GA91-9201-0004-00030 - 3E-GD-A0094 - Resolution Plan for RO-ABWR- 0031 SSLC and Support System Architecture.
155. Hitachi-GE UK ABWR - GA91-9201-0005-00030 - Rev 0 - 3E-GD-A01130 - Detailed Gantt Chart for UK ABWR Resolution Plan (Corresponding to RO-ABWR-0031).
156. Hitachi-GE UK ABWR - GA91-9201-0004-00031 - 3E-GD-A0088 - Rev 1 - Resolution Plan for RO-ABWR-0032 - Safety System Logic & Control (SSLC) Design.
157. Hitachi-GE UK ABWR - GA91-9201-0005-00031 - 3E-GD-A0114 - Rev 1 - Detailed Gantt Chart for UK ABWR Resolution Plan - Corresponding to RO-ABWR-0032.
158. Hitachi-GE UK ABWR - GA91-9201-0004-00061 - 3E-GD-A0199 - Rev 0 - Resolution Plan for RO-ABWR-0061 Reactor Pressure Vessel Instrumentation Connections.
159. Hitachi-GE UK ABWR - GA91-9201-0005-00061 - 3E-GD-A0219 - Rev 0 - Detailed Gantt Chart for UK ABWR Resolution Plan (Corresponding to RO-ABWR-0061).
160. Hitachi-GE UK ABWR - GA91-9201-0004-00062 - 3E-GD-A0200 - Rev 0 - Resolution Plan for RO-ABWR-0062 Testing and Maintenance of Safety Systems.
161. Hitachi-GE UK ABWR - GA91-9201-0005-00062 - 3E-GD-A0220 - Rev 0 - Detailed Gantt Chart for UK ABWR Resolution Plan (Corresponding to RO-ABWR-0062).
162. Hitachi-GE UK ABWR - GA91-9201-0003-02146 - AE-GD-0980 - Rev 0 - Technical Memorandum of Internal Fire at Power PSA Refinement.
163. Hitachi-GE, UK ABWR - GA91-9201-0002-00041 - HPE-GD-H006 - Rev 3 - Basis of Safety Cases on Heating Ventilating and Air Conditioning System.
164. RO-ABWR-0007 - Spurious C&I Failures as Design Basis Initiating Events.
165. ONR, ABWR - GDA Step 4 - Fault Studies - Assessment of response to RO-ABWR-007, TRIM 2016/354722.

# Annex 1

## Safety Assessment Principles

| SAP No | SAP Title | Description |
|---|---|---|
| EKP.3 | Defence in depth | Nuclear facilities should be designed and operated so that defence in depth against potentially significant faults or failures is achieved by the provision of multiple independent barriers to fault progression. |
| EKP.4 | Safety function | The safety function(s) to be delivered within the facility should be identified by a structured analysis. |
| EKP.5 | Safety measures | Safety measures should be identified to deliver the required safety function(s). |
| ECS.1 | Safety categorisation and standards | The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be identified and then categorised based on their significance with regard to safety. |
| 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 to safety. |
| ECS.3 | Codes and Standards | Structures, systems and components that are important to safety should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to the appropriate codes and standards. |
| ECS.4 | Absence of established codes and standards | Where there are no appropriate established codes or standards, an approach derived from existing codes or standards for similar equipment, in applications with similar safety significance, should be adopted. |
| EQU.1 | Qualification procedures | Qualification procedures should be applied to confirm that structures, systems and components will perform their allocated safety function(s) in all normal operational, fault and accident conditions identified in the safety case and for the duration of their operational lives. |
| EDR.1 | Failure to safety | Due account should be taken of the need for structures, systems and components 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 | Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components. |
| EDR.3 | Common cause failure | Common cause failure (CCF) should be addressed explicitly where a structure, system or component employs redundant or diverse components, measurements or actions to provide high reliability. |
| EDR.4 | Single failure criterion | During any normally permissible state of plant availability, no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function. |
| ERL.1 | Form of claims | The reliability claimed for any structure, system or component should take into account its novelty, experience |

| SAP No | SAP Title | Description |
|---|---|---|
| | | relevant to its proposed environment, and uncertainties in operating and fault conditions, physical data and design methods. |
| ERL.2 | Measures to achieve reliability | The measures whereby the claimed reliability of systems and components will be achieved in practice should be stated. |
| ERL.3 | Engineered safety measures | Where reliable and rapid protective action is required, automatically initiated, engineered safety measures should be provided. |
| EMT.1 | Identification of requirements | Safety requirements for in-service testing, inspection and other maintenance procedures and frequencies should be identified in the safety case. |
| EMT.2 | Frequency | Structures, systems and components should receive regular and systematic examination, inspection, maintenance and testing as defined in the safety case. |
| EMT.5 | Procedures | Commissioning and in-service inspection and test procedures should be adopted that ensure initial and continuing quality and reliability. |
| EMT.6 | Reliability claims | Provision should be made for testing, maintaining, monitoring and inspecting structures, systems and components (including portable equipment) in service or at intervals throughout their life, commensurate with the reliability required of each item. |
| EMT.7 | Functional testing | In-service functional testing of structures, systems and components should prove the complete system and the safety function of each functional group. |
| EMT.8 | Continuing reliability following events | Structures, systems and components should be inspected and/or re-validated after any event that might have challenged their continuing reliability. |
| EAD.1 | Safe working life | The safe working life of structures, systems and components that are important to safety should be evaluated and defined at the design stage. |
| EAD.2 | Lifetime margins | Adequate margins should exist throughout the life of a facility to allow for the effects of materials ageing and degradation processes on structures, systems and components. |
| ELO.1 | Access | The design and layout should facilitate access for necessary activities and minimise adverse interactions while not compromising security aspects. |
| ELO.2 | Unauthorised access | Unauthorised access to, or interference with, structures, systems and components or their reference data (including Building Information Modelling (BIM)) should be prevented. |
| ELO.4 | Minimisation of the effects of incidents | The design and layout of the site, its facilities (including enclosed plant), support facilities and services should be such that the effects of faults and accidents are minimised. |
| EHA.10 | Electromagnetic interference | The facility design should include preventative and/or protective measures against the effects of electromagnetic |

| SAP No | SAP Title | Description |
|---|---|---|
| | | interference. |
| ESS.1 | Provision of 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 stable, safe state. |
| ESS.2 | Safety system specification | The extent of safety system provisions, their functions, levels of protection necessary to achieve defence in depth and reliability requirements should be specified. |
| ESS.3 | Monitoring of plant safety | Adequate provisions should be made to enable the monitoring of the facility state in relation to safety and to enable the taking of any necessary safety actions during normal operational, fault, accident and severe accident conditions. |
| ESS.5 | Plant interfaces | The interfaces between the safety system and the plant to detect a fault condition and bring about a stable, safe state should be engineered by means that have a direct, known, timely and unambiguous relationship with plant behaviour. |
| ESS.6 | Adequacy of variables | Where it is not possible to use a directly related variable to detect a fault condition, the variable chosen should have a known relationship with the fault condition. |
| ESS.7 | Diversity in the detection of fault sequences | All Class 1 protection systems should employ diversity in their detection of and response to fault conditions, preferably by the use of different variables. |
| ESS.8 | Automatic initiation | For all fast acting faults (typically less than 30 minutes) safety systems should be initiated automatically and no human intervention should then be necessary to deliver the safety function(s). |
| ESS.10 | Definition of capability | The capability of a safety system, and of each of its constituent sub-systems and components, should be defined and substantiated. |
| ESS.11 | Demonstration of adequacy | The adequacy of the system design to achieve its specified functions and reliabilities should be demonstrated for each safety system. |
| ESS.12 | Prevention of service infringement | Adequate arrangements should be in place to prevent any infringement of the services supporting a safety system, its sub-systems or components |
| ESS.13 | Confirmation of operating personnel | There should be direct means of confirming to operating personnel: (a) that a demand for safety system action has arisen; (b) that the safety systems have operated (actuated) fully and correctly; and (c) whether any limiting condition (operating rule) has been exceeded which takes the safety system beyond its substantiated capability (see Principle ESS.10). |
| ESS.14 | Self-resetting of safety systems | Safety system actions and associated alarms should not be self-resetting, irrespective of the subsequent status of the initiating fault. |
| ESS.15 | Alteration of configuration, operational logic or associated data | No means should be provided, or be readily available, by which the configuration of a safety system, its operational logic or the associated data (trip levels etc) can be altered, other than by specifically engineered and adequately secured maintenance/testing provisions used under strict administrative control. |

| SAP No | SAP Title | Description |
|---|---|---|
| ESS.16 | No dependency on external sources of energy | Where practicable, following a safety system action, maintaining a stable, safe state should not depend on an external source of energy. |
| ESS.17 | Faults originating from safety systems | Potential faults originating from within safety systems (eg due to spurious or mal-operation) should be identified and protection against them provided. |
| ESS.18 | Failure independence | No design basis event should disable a safety system. |
| ESS.19 | Dedication to a single task | A safety system should be dedicated solely to the provision of its allocated safety functions. |
| ESS.20 | Avoidance of connections to other systems | Connections between any part of a safety system and a system external to the facility (other than to safety system support and monitoring features) should be avoided. |
| ESS.21 | Reliability | The design of safety systems should avoid complexity, apply a failsafe approach and incorporate means of revealing internal faults at the time of their occurrence. |
| ESS.22 | Avoidance of spurious actuation | Spurious actuation of safety systems should be avoided by means such as the provision of multiple independent divisions within the design architecture and majority voting. |
| ESS.23 | Allowance for unavailability of equipment | In determining the safety systems to be provided, allowance should be made for the potential unavailability of equipment. |
| ESS.25 | Taking safety systems out of service | The vetoing or the taking out of service of any safety system function should be avoided. |
| ESS.26 | Maintenance and testing | Maintenance and testing of a safety system should not initiate a fault sequence. |
| ESS.27 | Computer-based safety systems | Where the system reliability is significantly dependent upon the performance of computer software, compliance with appropriate standards and practices throughout the software development lifecycle should be established in order to provide assurance of the final design. |
| 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 secondary control or monitoring locations. |
| ESR.3 | Provision of controls | Adequate and reliable controls should be provided to maintain all safety-related plant parameters within their specified ranges (operating rules). |
| ESR.4 | Minimum operational equipment | The minimum control and instrumentation in each of the facility's permitted operating modes should be specified (operating rules) and its adequacy substantiated. |
| ESR.5 | Standards for equipment in safety-related systems | Where computers, programmable or non-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. |
| ESR.6 | Power supplies | Safety-related system control and instrumentation should be operated from power supplies whose reliabilities and availabilities are consistent with the safety functions being performed |

| SAP No | SAP Title | Description |
|---|---|---|
| ESR.7 | Communications systems | Adequate communications systems should be provided to enable information and instructions to be transmitted between locations on and, where necessary, off the site. The systems should provide robust means of communication during normal operations, fault conditions and severe accidents. |
| ESR.8 | Monitoring of radioactive material | Instrumentation should be provided to detect the leak or escape of radioactive material from its designated location and then to monitor its location and quantity. |
| ESR.9 | Response of control systems to normal plant disturbances | Control systems should respond in a timely, reliable and stable manner to normal plant disturbances without causing demands on safety systems. |
| ESR.10 | Demands on safety systems in the event of control system faults | Faults in control systems and other safety-related instrumentation should not cause an excessive frequency of demands on safety systems or take any safety system beyond its capability limits. |
| EES.1 | Provision | Essential services should be provided to ensure the maintenance of a safe plant state in normal operation and in fault and accident conditions. |
| EES.6 | Reliability of back-up sources | Back-up sources of essential services should be designed so that their reliability will not be prejudiced by adverse conditions in the services to which they provide a back-up, eg from common cause failures. |
| EHF.7 | User interfaces | Suitable and sufficient user interfaces should be provided at appropriate locations to provide effective monitoring and control of the facility in normal operations, faults and accident conditions. |
| ERC.2 | Shutdown systems | At least two diverse systems should be provided for shutting down a civil reactor. |

## Annex 2

Technical Assessment Guides

| TAG Ref | TAG Title |
|---|---|
| NS-TAST-GD-003 Revision 7 | Safety Systems |
| NS-TAST-GD-005 Revision 7 | Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable) |
| NS-TAST-GD-046 Revision 4 | Computer based safety systems |
| NS-TAST-GD-049, Revision 5 | Licensee Core and Intelligent Customer Capabilities |
| NS-TAST-GD-051 Revision 4 | The purpose, scope, and content of safety cases, |
| NS-TAST-GD-077, Revision 3 | Supply Chain Management Arrangements for the Procurement of Nuclear Safety Related Items or Services |
| NS-TAST-GD-094 Revision 0 | Categorisation of safety functions and classification of structures, systems and components |

# Annex 3

National and International Standards and Guidance

| Key National & International Standards and Guidance used in the assessment |
|---|
| IEC 61513:2011, Nuclear power plants – Instrumentation and control important to safety – General requirements for systems. |
| IEC 61226:2009, Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions. |
| IEC 62566:2012, Nuclear power plants — Instrumentation and control important to safety — Development of HDL-programmed integrated circuits for systems performing category A functions. |
| IEC 60880:2006, Nuclear power plants. Instrumentation and control systems important to safety. Software – Software aspects for computer-based systems performing category A functions. |
| IEC 62138:2004, Nuclear power plants — Instrumentation and control important for safety — Software aspects for computer-based systems performing category B or C functions. |
| IEC 60987:2013, Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems. |
| IEC 62340:2007, Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF). |
| IEC 60709:2004, Nuclear power plants – Instrumentation and control systems important to safety – Separation. |
| IEC 60671:2007, Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing. |
| IEC 61500:2009, Nuclear power plants – Instrumentation and control important to safety – Data communications in systems performing category A functions. |
| IEC 62671:2013, Nuclear power plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality. |
| IEC 60964:2009, Nuclear power plants - Control Rooms – Design. |
| IEC 60965:2016, Nuclear power plants - Control Rooms - Supplementary control room for reactor shutdown without access to the main control room. |
| IEC/IEEE 60780-323:2016, Nuclear facilities – Electrical equipment important to safety – Qualification. |
| IEC 60980:1989, Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations. |
| IEC 61508:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems. |
| IEC 61000 series, Electromagnetic compatibility EMC (in 6 parts). |
| IAEA Safety Standards, Design of Instrumentation and Control Systems for Nuclear Power Plants, Specific Safety Guide SSG-39, 2016. |

| |
|---|
| IAEA Safety Standards, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, Specific Safety Guide SSG-30 2014 |
| Licensing of safety critical software for nuclear reactors. Common position of international nuclear regulators and authorised technical support organisations. Revised 2015. www.onr.org.uk/software.pdf |
| United States Nuclear Regulatory Commission, “Method for Performing Diversity and Defence-in-Depth Analyses of Reactor Protection Systems”, NUREG/CR-6303 (UCRLID-119239), 1994. |
| EEMUA 191 Alarm systems - a guide to design, management and procurement, 2013. |
| Generic Common Position DICWG-01: Common Position on the Treatment of Common Cause Failure Caused by Software within Digital Safety Systems. |
| Generic Common Position DICWG-02: Software Tools |
| Generic Common Position DICWG-03: Verification and Validation throughout the Life Cycle of Safety Systems Using Digital Computers |
| Generic Common Position DICWG-04: Communication Independence |
| Generic Common Position DICWG-05: Treatment of Hardware Description Language (HDL) Programmed Devices for Use in Nuclear Safety Systems |
| Generic Common Position DICWG-06: Simplicity in Design |
| Generic Common Position DICWG-07: Selection and Use of Industrial Digital devices of Limited Functionality (Update of 20 November 2014) |
| Generic Common Position DICWG-08: Impact of Cyber Security Features on Digital I&C Safety Systems |
| Generic Common Position DICWG-09: Safety Design Principles and Supporting Information for the Overall I&C Architecture |
| Generic Common Position DICWG-10 : Hazard Identification and Control for Digital Instrumentation and Control Systems |
| Generic Common Position DICWG-11: Digital I&C System Pre-installation and Initial On-site Testing |
| Generic Common Position DICWG-12: Use of Automatic Testing in Digital I&C Systems as part of Surveillance Testing |
| Generic Common Position DICWG-13: Common Position on Spurious Actuation |

## Annex 4

Regulatory Observations

| RO reference and topic | RO description and summary of assessment conclusions | Information related to the regulatory assessment of this RO |
|---|---|---|
| RO-ABWR-0026<br><br>Back-up Building Control and Instrumentation | **RO description**<br>The back-up building (BuB) has an important role in the safety of the UK ABWR. Its original role was to provide diverse support for beyond design basis accident sequences and severe accident sequences. Recent work on fault studies has shown that that the BuB also requires to cover a class of infrequent design basis events. The scope of the functional safety role of the control and instrumentation (C&I) proposed for the BuB is fully covered in Revision A of the UK ABWR PCSR. The purpose of this regulatory observation is to provide Hitachi-GE with guidance on ONR's expectations for the safety justification of the BuB C&I.<br><br>Action 1: Provide a high level description in Chapter 14 of the C&I located in the Back-up Building including good references to the derivation of the plant safety functions in the accident analysis chapters.<br><br>Action 2: Provide a Basis for Safety Case with supporting references on the Back-up building C&I.<br><br>**Summary of assessment conclusions**<br>I assessed the submissions relating to this RO and concluded that Hitachi-GE has provided the suitable documentation for the safety case and safety justification of the Backup Building C&I systems. | The Resolution Plan for this RO is Ref. 144 and the detailed Gantt chart is Ref. 145.<br><br>Section 4.2.3 in this report<br><br>Assessment note supporting the RO closure in Ref. 23 |
| RO-ABWR-0027<br><br>Hardwired Back-up System | **RO description**<br>Hitachi-GE's Step 2 Preliminary Safety Report (PSR) and the Chapter 14 of the Pre-Construction Safety Report (PCSR) provides high level information relating to the design of the Hardwired Backup safety System. The information is limited to describing the extent of the safety functions it provides and a brief description of the technology that will be used to implement these functions.<br>The Basis of Safety Case (BSC) for the Hardwired Backup System (GA91-9201-0002-00029 - 3D-GD-A0009 - Rev 0) provides further information than provided in the PSR and PCSR but does not give a full description of the overall system. Both reports and the BSC indicate that the UK ABWR Hardwired Backup System will consist of hardwired relay logic and trip amplifiers and will be diverse from the Safety System Logic and Control (SSLC) system.<br>During Step 2 a Regulatory Query (RQ) was raised (RQ-ABWR-0273) requesting clarification of what technology would be used for the Hardwired Backup System. The response to this RQ (GA91-9201-0003-00112) indicated that<br>"*The selection of the hard wired backup system technology is still to be confirmed. The current intention is to use analogue Trip Units and relay logic for voting. The inter connections will be hard wired.*"<br>The current C & I safety case submissions or information provided in the response to RQ-ABWR-0273 does not include sufficient information on the overall design of the Hardwired Backup System, the technology the system will be based on and how the design will address common cause and systematic failures (refer to IEC 61508). The purpose of this regulatory observation is to provide guidance on the regulatory expectations of the design and extent of the Hardwired Backup System. | The Resolution Plan for this RO is Ref. 146 and the detailed Gantt chart is Ref. 147.<br><br>Section 4.2.3 in this report<br><br>Assessment note supporting the RO closure in Ref. 24 |

| RO reference and topic | RO description and summary of assessment conclusions | Information related to the regulatory assessment of this RO |
|---|---|---|
| | Action 1: Hitachi-GE are to develop a comprehensive list of safety function requirements for the hardwired backup systems which are linked to the UK ABWR Fault Schedule.<br><br>Action 2: Hitachi-GE are to develop suitable documentation that describes the design, design process and potential technology used for the hardwired backup system and how the design protects against common cause and systematic failures. This should describe what design attributes the hardwired backup system must have to demonstrate common cause and systematic errors relating to other C&I safety systems will be avoided, including interfaces with those systems. An outline architecture drawing of the system should also be included.<br><br>**Summary of assessment conclusions**<br>I assessed the submissions relating to this RO and concluded that Hitachi-GE have suitable documentation that includes a comprehensive list of safety function requirements and description of the design, design process and potential technology used for the HWBS; and how the common cause and systematic failures between platforms with different classifications are minimised or avoided. | |
| RO-ABWR-0028<br><br>Safety System Logic & Control (SSLC) Class 1 HMI | **RO description**<br>Hitachi-GE's Step 2 Preliminary Safety Report (PSR) and Chapter 14 of the Pre-Construction Safety Report (PCSR) provides high level information relating to the design of the Human Machine Interfaces (HMI)s. The information is limited to describing the type, location and some high-level functions that are performed using the HMI for individual systems. Both reports indicate that the UK ABWR Safety System Logic and Control (SSLC) system, which has a safety Classification of 1, has a HMI connected to it. The function of this HMI is not fully described but both reports state that it is a "Flat Display". During technical meetings and a visit to Hitachi Omika works it has become evident to ONR that the SSLC Flat Display uses touch screen technology as one means for the plant operator to interact with the safety system.<br>During Step 2 a Regulatory Query (RQ) was raised (RO-ABWR-0028) requesting clarification that the classification of the SSLC HMI was commensurate with the SSLC classification. The response to this RQ (GA91-9201-0003-00112) indicated there is two way communications between Flat Display Panels and the SSLC for the Main Control Console and the Wide Display Panel. The RQ response goes on to state that it is Hitachi-GE's intention to;<br>"*make the local the operator interface such that its connection to the Class 1 SSLC is commensurate with the overall classification of the system. The nature of the interface has not been determined and a study into the nature of the operator interface is currently being undertaken*".<br>The current C & I safety case submissions or information provided in the response to RO-ABWR-0028 does not include sufficient information on how Hitachi-GE propose to provide a Class 1 HMI for the SSLC. The purpose of this regulatory observation is to provide guidance on the regulatory expectations of the HMI for the Class 1 SSLC.<br><br>Action 1: Hitachi-GE are to develop suitable documentation that describes the functionality of the SSLC HMI. This should include a description of the high-level functionality and the modes of operation in which the HMI is used. References should be included to Human Factors documentation. | The Resolution Plan for this RO is Ref. 148 and the detailed Gantt chart is Ref. 149.<br><br>Section 4.2.5.2 in this report<br><br>Assessment note supporting the RO closure in Ref. 25 |

| RO reference and topic | RO description and summary of assessment conclusions | Information related to the regulatory assessment of this RO |
|---|---|---|
| | Action 2: Hitachi-GE are to develop suitable documentation that describes the design of the SSLC HMI and the selected technology. This should include a high-level description of how the design protects against fault propagation and corruption of information.<br><br>Action 3: Hitachi-GE are to develop suitable documentation that justifies the technology selected for the SSLC HMI. An important part of the justification will be an initial high-level compliance analysis against standards such as IEC 61513. This analysis should be focused on the architectural aspects.<br><br>**Summary of assessment conclusions**<br>I assessed submissions relating to this RO and concluded that Hitachi-GE has developed suitable documentation that describes the high level functionality and modes of operation of the HMI, including human factors, that a feasible design has been established using the selected technology that protects against fault propagation and corruption of information, and that the selected technology and its architecture have been justified using analysis against relevant standards. Touch screen technology is not used in the Class 1 SSLC HMI. | |
| RO-ABWR-0029<br><br>SSLC Production Excellence | **RO description**<br>The UK ABWR's Safety System Logic and Control (SSLC) is the main safety class 1 control and instrumentation (C & I) system performing the safety functions of reactor trip and essential safety feature actuations. To meet ONR's expectations on diversity the platform technology for the SSLC will be based on field programmable gate arrays (FPGA) supported by other more conventional integrated and discrete electronic circuits. Techniques for the design of FPGA technology has many similarities with that of the design of software for computer based safety systems, meaning that ONR's expectations for the safety demonstration of production excellence is given in ONR's technical assessment guide 46 (http://www.onr.org.uk/operational/tech_asst_guides/index.htm). This regulatory observation provides further guidance on the application of TAG 46 specifically on the topic of production excellence for the FPGA based SSLC. For Step 3 this RO is seeking a topic report describing and justifying the methodologies selected by Hitachi-GE.<br><br>Action 1: Hitachi-GE to develop a suitable document(s) describing and justifying the methodology for developing the production excellence leg of the SSLC platform design.<br><br>Action 2: Hitachi-GE should identify how and what information it will provide to allow a third party to design a test oracle and harness to conduct statistical testing, this should include all the information required to enable an oracle to be designed.<br><br>**Summary of assessment conclusions**<br>I assessed submissions relating to this RO and concluded that Hitachi-GE has developed suitable documentation that describes the methodology for developing the production excellence leg of the SSLC platform design, and that the RP Hitachi-GE has identified information suitable to design a statistical testing harness and oracle. | The Resolution Plan for this RO is Ref. 150 and the detailed Gantt chart is Ref. 151.<br><br>Section 4.2.3 in this report<br><br>Assessment note supporting the RO closure in Ref. 26 |
| RO-ABWR-0030<br><br>Embedded C&I | **RO description**<br>Many support systems important to safety for the UK ABWR will have embedded control and instrumentation (C & I) subsystems and smart devices. The correct operation of these will be critical for the achievement of the safe operation of the UK ABWR. | The Resolution Plan for this RO is Ref. 152 and the detailed Gantt chart |

| RO reference and topic | RO description and summary of assessment conclusions | Information related to the regulatory assessment of this RO |
|---|---|---|
| subsystems and smart devices | Typical support systems important to safety employing C&I based embedded subsystems include heating and ventilation, chilled water, electrical power, variable speed drives, complex plant sensors and plant actuators.<br>The current safety submission for the UK ABWR does not cover these important embedded C&I subsystems and the purpose of this regulatory observation is to provide guidance on their identification and safety justification.<br>Appendix 1 of this RO gives a definition of embedded control and instrumentation subsystems and smart devices.<br><br>Action 1: Hitachi-GE are to derive a list of embedded SC1 and SC2 C&I systems which clearly identifies the use of smart devices based on the analysis of<br>n RO 8 and RO 10.<br>n Knowledge of the location of other sources of smart devices as sensors, actuators and variable speed drives used in SC1 and SC2 systems throughout the facility.<br><br>Action 2: Hitachi-GE are to develop a topic report on their proposed approach to the assessment of the production excellence of all smart devices and to give recommendations to a future licensee on methods of independent confidence building.<br><br>Action 3: From the outcome of action 2 Hitachi-GE are to develop a topic report demonstrating the viability of the production excellence and independent confidence building process by applying these methods to one SC1 and one SC2 devices taken from the list derived in action 1.<br><br>**Summary of assessment conclusions**<br>I assessed the submissions relating to this RO and concluded that, through the response to these RO actions, Hitachi-GE has developed an adequate understanding of the UK expectation for smart device justification. An assessment finding was raised to address some related aspects which lay outside GDA. | is Ref. 153.<br><br>Section 4.2.5 in this report<br><br>Assessment note supporting the RO closure in Ref. 27 |
| RO-ABWR-0031<br><br>SSLC and Support System Architecture | **RO description**<br>The UK ABWR safety system logic and control (SSLC) is a Class 1 safety system providing control for the actuation of the UK ABWR plant level category A safety functions. In line with international standards, its internal architecture is a four-division safety system with majority voting to undertake a wide range of safety actuations such as reactor trip. There are a number of plant level safety functions that do not utilise all four safety divisions and some of which appear to fail to meet the single failure criterion at the system level. The purpose of this Regulatory Observation is to seek a safety justification for the architecture of the support systems actuated by the SSLC, particularly the fact that some of the essential safety feature (ESF) actuations are controlled by two divisions of equipment at the safety logic unit (SLU) level which contrast with higher level of SLU redundancy (three or four divisions) for other safety functions. This RO is a joint one between C&I and fault studies as the ONR's challenge is on the adequacy of the delivery systems (for example automatic depressurisation) as well as the C&I (SSLC) controlling the actuation of the safety function.<br><br>Action 1: Hitachi-GE should review and assign a safety functional category to all of the SSLC plant level functions. A list of safety function and category should be submitted to ONR for assessment. | The Resolution Plan for this RO is Ref. 154 and the detailed Gantt chart is Ref. 155.<br><br>Section 4.2.4 in this report<br><br>Assessment note supporting the RO closure in Ref. 28 |

| RO reference and topic | RO description and summary of assessment conclusions | Information related to the regulatory assessment of this RO |
|---|---|---|
| | Action 2: Where the functions listed above are assigned to a category A safety function then ONR's expectation is that they are designed to follow an N+2 format consistent with the ECCS and therefore the SSLC and the systems it is actuating are modified accordingly. Where the functions are category B or lower then a safety justification should be provided why the SSLC is used for a lower safety functional category role. Where category B is required and two divisions or lower is retained then full justification that no failure in this reduced architecture (dual or single division) could interfere with the operation of the whole four divisional SSLC. Hitachi-GE should identify, and submit a document that descibes any design changes that are required to comply with the expectations set out in the RO.<br><br>**Summary of assessment conclusions**<br>I assessed the submissions relating to this RO and, with the opinions from the Fault Studies' assessor, concluded that Hitachi-GE has developed suitable documentation which provided adequate justification for the architectural design of these Class 1 safety functions. In addition to that, Hitachi-GE have designed a separate C&I system for the lower class safety functions to provide the independence between the Class 1 and the lower class safety functions. | |
| RO-ABWR-0032<br><br>Safety System Logic Control (SSLC) Design | **RO description**<br>Hitachi-GE's Step 2 Preliminary Safety Report (PSR) and Chapter 14 of the Pre-Construction Safety Report (PCSR) provides high level information relating to the design processes that will be used during the development of the Control and Instrumentation (C & I) systems for the UK ABWR. In particular these documents provide a high level outline of the lifecycle approach to the design of C & I systems by briefly describing the stages of the process. The information is generic in nature and could be applied to any C & I system. During Step 2 of the Generic Design Assessment (GDA) Hitachi-GE committed to modify the platform technology for the main safety class 1 Safety System Logic and Control (SSLC). This commitment was given to improve the diversity of this system from the other major C & I platforms by developing a new platform based on Field Programmable Gate Array (FPGA) technology. The proposed design of the FPGA based SSLC will therefore be new and its design will need to follow a defined process that is commensurate with its deterministic and probabilistic safety claims.<br><br>The current C & I safety case submissions do not cover the specific design and development processes for the FPGA based SSLC. The purpose of this regulatory observation is to provide guidance on the regulatory expectations of the design and development process for the new design SSLC.<br><br>Action 1: Hitachi-GE are to develop suitable documentation that describes the design and development process for the FPGA based SSLC and supports this with an Activity Schedule that demonstrates the design will be sufficiently complete by the end of GDA to enable ONR to complete its assessment. The description should include the rationale why Hitachi-GE believes the process is suitable for the design and development of a Class 1 FPGA safety system.<br><br>Action 2: Hitachi-GE to demonstrate that the design team for the SSLC is effectively independent from other C & I system design teams and that the independence is included in relevant design and development processes and procedures. | The Resolution Plan for this RO is Ref. 156 and the detailed Gantt chart is Ref. 157.<br><br>Section 4.2.3 in this report<br><br>Assessment note supporting the RO closure in Ref. 29 |

| RO reference and topic | RO description and summary of assessment conclusions | Information related to the regulatory assessment of this RO |
|---|---|---|
| | **Summary of assessment conclusions**<br>I concluded, through my assessment of relevant GDA submissions, that Hitachi-GE has developed suitable documentation that describes the design and development process for the Class 1 SSLC. The design and development process has been used to produce prototype SSLC modules, and the validation and verification processes have been demonstrated to be feasible and effective through the submission of suitable evidence documentation. The adequacy of the design and development process for a Class 1 system has been demonstrated through the submission of safety case documentation that uses a CAE structure to argue that the relevant standards and regulatory expectations have been met by means of compliance assessments and other analyses.<br>I judged that the design team for the SSLC has been, and remains, effectively independent of other C&I teams as a result of the organisational structure of the RP Hitachi-GE, and that this is adequately reflected in documentation. | |
| RO-ABWR-0061<br><br>Reactor Pressure Vessel Instrumentation Connections | **RO description**<br>During Step 2 of the Generic Design Assessment (GDA) of the UK Advanced Boiling Water Reactor (ABWR) an area to follow up during Step 3 was identified (see ONR Step 2 UK ABWR Control and Instrumentation Assessment Report ONR-GDA-AR-14-006). This area was related to the sharing of instrumentation connection lines, often referred to as instrument impulse lines, by the Primary Protection System (SSLC), Secondary Protection System (HWBS) and Plant Control System (PCntlS) to the Reactor Pressure Vessel (RPV). The particular concern being the potential susceptibility of the proposed design to common cause failure of the four lines that would affect all divisions of the three main Control and Instrumentation (C & I) systems simultaneously. The SSLC design proposed for the UK ABWR is based on a four division design with four sets of instrument impulse lines providing the means of connection to the RPV. The four sets of RPV impulse lines are also shared by the HWBS and the PCntlS.<br>ONR's assessment during Step 3 has revealed further information relating to the instrumentation impulse line connections, in particular their use for additional instrumentation associated with the automation of some of the Secondary Protection System safety functions which may also be connected to the RPV impulse lines.<br>During Step 3 Hitachi-GE issued a Topic Report on the Reactor Pressure Vessel Instrument System (GA91-9201-0001-00056) which states within Section 3.1;<br>*"Common pressure taps / sensing lines are used for a number of the sensors in order to minimise the number of penetrations of the reactor pressure vessel"*<br>Further information is provided in Fig. 3.1-1 of GA91-9201-0001-00056 which diagrammatically shows the instrumentation connections of the Safety Class 1 and 2 instruments and other instrumentation.<br>The current C & I safety case submission does not include adequate justification for the use of common RPV instrumentation impulse lines and how common cause failures are protected against. ONR is aware that Hitachi-GE is currently reviewing the design of the RPV impulse lines and is undertaking an optioneering exercise. The purpose of this regulatory observation is to provide guidance on the regulatory expectations of the connection of instrumentation to the RPV.<br><br><u>Action 1</u>: Hitachi-GE are to develop suitable documentation that includes a description of the optioneering studies that have been carried out to determine the form of the RPV instrumentation lines used for pressure and level measurement. The optioneering should address how specifically common cause failures have addressed in respect of the impact on pressure and level measurement and impact on the three major C & I systems. | The Resolution Plan for this RO is Ref. 158 and the detailed Gantt chart is Ref. 159.<br><br>Section 4.2.3 in this report<br><br>Assessment note supporting the RO closure in Ref. 30 |

| RO reference and topic | RO description and summary of assessment conclusions | Information related to the regulatory assessment of this RO |
|---|---|---|
| | Action 2: Hitachi-GE are to develop suitable documentation that substantiates the proposed design of the RPV Instrumentation System in respect of C & I including the consequences of common cause failure. It is expected that the documentation will follow the claims, arguments and evidence approach.<br><br>Action 3. Hitachi-GE should confirm that the proposed design of the RPV impulse lines has been included in the safety cases for all affected topic areas including structural integrity, mechanical engineering, Fault Studies and PSA.<br><br>**Summary of assessment conclusions**<br>I assessed the submissions relating to this RO, and with the opinions from the relevant disciplines assessors, and concluded that Hitachi-GE have performed adequate optioneering and that the selected option reduces the risk of CCF so far as is reasonably practicable. This has resulted in design changes to the instrumentation sensing lines both outside and inside of the RPV, in addition to the requirement for using different technologies amongst the three different Safety Classes C&I systems | |
| RO-ABWR-0062<br><br>Testing and Maintenance of Safety Systems | **RO description**<br>During Step 3 of the UK advanced Boiling Water Reactor (ABWR) Control and Instrumentation (C & I) Generic Design Assessment (GDA) the approach to testing and maintenance of safety systems has been discussed. In particular the testing and maintenance while the nuclear power plant (NPP) is at power. Hitachi-GE have presented the method used for testing and maintaining ABWR safety systems in Japan and the proposed approach for the UK ABWR which aligns with the Japanese method with regard to the methodology and test frequency.<br>Chapter 14 of Hitachi-GE's Pre-Construction Safety Report (PCSR) (GA10-9101-0101-14000 Rev A) provides high level information relating to the Testing of Safety Systems. The PCSR sets out the high-level requirements for the design of the C & I Architecture and the platforms and systems that it comprises of. Chapter 14 includes summary descriptions of the test and maintenance facilities for C & I systems and links these requirements to Japanese national standards and guides (JEAC and JAEG), international standards and guides (IEC and IAEA) and to the ONR Safety Assessment Principles (SAPs). The PCSR references other supporting documentation in the form of Basis of Safety Cases (BSC)s for C & I safety systems.<br>Sections 14.5.2, 14.5.2.1 and 14.5.2.2 of Chapter 14 of the PCSR identify specific design features and requirements for the testing and maintenance of the Safety System Logic and Control (SSLC) system. These include Reactor Protection System (RPS), Emergency Core Cooling System (ECCS), Emergency Safety Features (ESF)<br><br>Action 1: Hitachi-GE are to develop suitable documentation that describes and substantiates the methodology to testing and maintenance of safety systems. It is expected that the documentation will follow the claims, arguments and evidence approach and this will include the identification and justification of the cases where the system / part system under test can re-aligne itself in response to a demand during testing.<br><br>Action 2: Hitachi-GE should confirm to ONR that the proposed methodology for testing and maintenance of safety systems has been included in the safety case for all related topic areas; e.g. mechanical and electrical engineering, and that it has been correctly accounted for (modelled in) the PSA and related fault studies. | The Resolution Plan for this RO is Ref. 160 and the detailed Gantt chart is Ref. 161.<br><br>Section 4.2.7 in this report<br><br>Assessment note supporting the RO closure in Ref. 31 |

| RO reference and topic | RO description and summary of assessment conclusions | Information related to the regulatory assessment of this RO |
|---|---|---|
| | Action 3: Hitachi-GE should confirm that the methodology for testing and maintenance has been clearly communicated to the prospective licensee of the UK ABWR.<br><br>**Summary of assessment conclusions**<br>I assessed the submissions relating to this RO, and found that the relevant factors to be considered in setting the maintenance and test interval for a range of different equipment types have now been identified and adequately documented. The methodology for testing and maintenance is described in PCSR chapter 5, and references UK good practice and describes the purpose of maintenance and testing in a technology neutral manner. I judge that the overall methodology for testing and maintenance will be adequately communicated to the prospective licensee through the documentation. However, no suitable document could be found to describe the factors affecting testing and maintenance intervals, so Hitachi-GE produced entry COM_SR.1 in the assumption management database to be acted upon by the future licensee. The actions of this RO have been completed to my satisfaction. | |

## Annex 5

Assessment Findings

| Assessment Finding Number | Assessment Finding[1] | Report Section and Technical Observation Reference[2] |
|---|---|---|
| AF-UKABWR-CI-001 | During GDA, Hitachi-GE has demonstrated to ONR's satisfaction that the key principles in the relevant nuclear standards are considered in the UK ABWR C&I design and safety case. Post GDA, ONR's expectation is for this exercise to be extended to all of the relevant C&I systems that were out of scope of GDA, and to further develop the work by considering the detailed design information and, if necessary, justifying whether any clause in the standards is considered not applicable. The expectation is that this should be carried out as part of the consolidation of the system attributes (i.e. the safety property claims in Hitachi-GE nomenclature) identified in the UK ABWR C&I safety case.<br><br>The licensee shall:<br>a. Produce a demonstration of compliance to relevant international nuclear sector C&I standards, for UK ABWR C&I systems and for the overall architecture as appropriate.<br>b. Develop an appropriate methodology to identify any potential gaps in the safety property claims, and apply this across the C&I systems in the UK ABWR architecture. | Section 4.2.1 of this report and TSCRep2-TO2-2.5.4-3, TSCRep2-TO2-2.6.4-2, TSCRep2-TO2-2.6.4-7 in Ref. 33. |
| AF-UKABWR-CI-002 | During GDA, a number of observations relating to the C&I safety case were identified in the C&I assessment. These are not considered to present an impediment to the closure of GDA, but they should be reviewed, and as appropriate, taken into account in detailed design and site-specific safety case development work post-GDA. Because these observations resulted from a sampling of the safety submissions, ONR's expectation is that they should be addressed considering the wider implication on the C&I documentation and that suitable arrangements are put in place to ensure the clarity and consistency of future revisions of the C&I safety case.<br><br>The licensee shall:<br>a. Develop a strategy for the appropriate resolution of the technical observations made in GDA Step 4 as part of the further development of the C&I safety case for the UK ABWR. | Section 4.2.1 in this report and TSCRep2-TO2-2.2.4-1, TSCRep2-TO2-2.2.4-2, TSCRep2-TO2-2.5.4-1, TSCRep2-TO2-2.5.4-2, TSCRep2-TO2-2.5.4-4, TSCRep2-TO2-2.1.4-4, TSCRep2-TO2-2.3.4-2, TSCRep2-TO2-2.4.4-1, TSCRep2-TO2-2.4.4-2, TSCRep3-TO2-2.1.4.1-1 , TSCRep1-TO2-2.1.4-1, TSCRep1-TO2-2.1.4-2, TSCRep1-TO2-2.3.4-1, TSCRep1-TO2-2.6.4-1, TSCRep2-TO2-2.1.4-5, TSCRep2-TO2-2.6.4-5, TSCRep2-TO2-2.6.4-6, TSCRep2-TO2-2.2.4-3, TSCRep4-TO2-2.1.4-1, TSCRep4-TO2-2.2.4-1, TSCRep4-TO2-2.2.4-2, TSCRep4-TO2-2.2.4-3, TSCRep4-TO2-2.2.4-4, TSCRep4-TO2-2.2.4-8, TSCRep4-TO2-2.2.4-13, TSCRep4-TO2- |

[1] The assessment findings should be considered in the context defined in relevant sections of the report, which provide their justification/significance and clarify the expectation for their resolution.
[2] As clarified in Section 4.8 of the report, the TO2s should be considered as examples of observations arising from the review of Hitachi-GE submissions performed on sampling basis and, for this reason, they should be addressed considering the wider implications on the overall safety case.

| Assessment Finding Number | Assessment Finding[1] | Report Section and Technical Observation Reference[2] |
|---|---|---|
| | | 2.3.4-1, TSCRep4-TO2-2.3.4-2, TSCRep4-TO2-2.3.4-4, TSCRep4-TO2-2.3.4-8, TSCRep4-TO2-2.3.4-9, TSCRep4-TO2-2.4.4.2-2, , TSCRep4-TO2-2.4.4.2-6, , TSCRep4-TO2-2.4.4.4-1, TSCRep4-TO2-2.4.4.4-3, TSCRep4-TO2-2.5.4.1-1, TSCRep4-TO2-2.5.4.3-1, TSCRep4-TO2-2.6.4-1, TSCRep4-TO2-2.6.4-2, TSCRep4-TO2-2.6.4-3, TSCRep4-TO2-2.6.4-4, TSCRep4-TO2-2.6.4-5, TSCRep4-TO2-2.7.4.1-2, TSCRep4-TO2-2.7.4.5-2, TSCRep5-TO2-2.3.4-1, TSCRep5-TO2-2.3.4-3, TSCRep5-TO2-2.3.4-4 , TSCRep5-TO2-2.4.4-2, TSCRep5-TO2-2.4.4-1, TSCRep5-TO2-2.5.4-1, TSCRep5-TO2-2.5.4-2, TSCRep5-TO2-2.6.4-1, TSCRep3-TO2-2.2.4.2-1, TSCRep3-TO2-2.2.4.2-4, TSCRep3-TO2-2.2.4.4-1, TSCRep3-TO2-2.6.4.2-1, TSCRep3-TO2-2.6.4.3-1, TSCRep3-TO2-3.3.2-1, TSCRep3-TO2-3.4.2-1, TSCRep3-TO2-3.5.2.2-1, TSCRep3-TO2-3.8.2-1, TSCRep3-TO2-4.3.2-1, TSCRep3-TO2-4.4.2-1, TSCRep3-TO2-4.5.4-1, TSCRep3-TO2-2.2.4.3-3, TSCRep3-TO2-3.7.2-1, TSCRep4-TO2-2.5.4.2-1, TSCRep4-TO2-2.2.4-1, TSCRep1-TO2-2.5.4-3, TSCRep1-TO2-2.5.4-5, TSCRep1-TO2-2.5.4-1, TSCRep1-TO2-2.5.4-2, TSCRep1-TO2-2.5.4-4, TSCRep5-TO2-2.7.4-1, TSCRep5-TO2-2.7.4-2 in Refs. 32-36. |
| AF-UKABWR-CI-003 | During GDA, Hitachi-GE provided adequate submissions regarding the suitability of the vCOSS®/NCFS-1 platform for use at safety class 1. In the safety case provided in GDA, in several instances Hitachi-GE referred to the evidence relating to the safety class 1 platform for the whole SSLC system (including the | Section 4.2.1 in this report and TSCRep4-TO2-2.2.4-5, TSCRep4-TO2-2.2.4-6, TSCRep4-TO2-2.2.4-9, |

[1] The assessment findings should be considered in the context defined in relevant sections of the report, which provide their justification/significance and clarify the expectation for their resolution.
[2] As clarified in Section 4.8 of the report, the TO2s should be considered as examples of observations arising from the review of Hitachi-GE submissions performed on sampling basis and, for this reason, they should be addressed considering the wider implications on the overall safety case.

| Assessment Finding Number | Assessment Finding[1] | Report Section and Technical Observation Reference[2] |
|---|---|---|
| | application). Until the final SSLC system requirement specifications have been fully determined during detailed design, it will not be possible to confirm that the substantiation at platform level is adequate at the system level.<br><br>The licensee shall assess and adequately report on the suitability of proposed class 1 platform to support the system level requirements for the SSLC. | TSCRep4-TO2-2.2.4-11, TSCRep4-TO2-2.2.4-12, TSCRep4-TO2-2.3.4-5, TSCRep4-TO2-2.7.4.1-1 in Ref. 35. |
| AF-UKABWR-CI-004 | During GDA Step 4, Hitachi-GE provided a justification for the PCntlS being safety class 3 following a period earlier in GDA where inconsistent documentation implied the classification was safety class 2. This justification of the PCntlS as safety class 3, based on standards, deterministic and probabilistic arguments is considered acceptable for GDA. However, ONR's expectation post GDA is that further verification work is undertaken, based on the more detailed design information that will be available, to confirm that the PCntlS safety classification is correct and appropriately reflected in the UK ABWR safety case.<br><br>The licensee shall ensure consistency in the classification of the PCntlS and its justification throughout the whole C&I safety case, including:<br>a. A safety assessment of the impact of aligning the documentation of the PCntlS safety classification across all safety case documentation.<br>b. A justification of the robustness of the PCntlS against faults which could cause spurious actuations, including multiple spurious actuations, considering:<br>• The PCntlS architecture and data flow.<br>• The effect of the use of multiple common components.<br>• The measures deployed to manage the effects of failures. | Section 4.2.2 of this report and TSCRep4-TO2-2.9.4.5-1, TSCRep4-TO2-2.9.4.5-2, TSCRep4-TO2-2.9.4.6-1 from Ref. 35. |
| AF-UKABWR-CI-005 | During GDA, Hitachi-GE provided sufficient evidence that principles are in place to confirm adequate diversity between the main C&I systems (e.g. including technology, human and equipment diversity). Post GDA, ONR's expectation is that the detailed design information is used to complete the diversity demonstration.<br><br>Where claims of diversity are made between C&I systems, the licensee shall complete diversity analyses by using the detailed design information (including sensors, actuators, and supporting systems). This should expand upon the approach applied in GDA, based on NUREG CR/6303, by taking account of other relevant diversity standards and guidance (e.g. IEC 62340 and the regulator consensus document 'Licensing of safety critical software for nuclear reactors'). | Section 4.2.2 of this report and TSCRep2-TO2-2.3.4-1 from Ref. 33. |
| AF-UKABWR-CI-006 | During GDA some differences were identified between the reliability figures used in the PSA and in the C&I substantiation in the safety case. As the PSA model evolves post GDA, ONR's expectation is that the reliability data should align to ensure a realistic estimation of the risk from the plant, unless there is a | Section 4.2.2 of this report and TSCRep4-TO2-2.2.4-10, TSCRep4-TO2-2.3.4-3, TSCRep4-TO2-2.3.4-6, |

[1] The assessment findings should be considered in the context defined in relevant sections of the report, which provide their justification/significance and clarify the expectation for their resolution.
[2] As clarified in Section 4.8 of the report, the TO2s should be considered as examples of observations arising from the review of Hitachi-GE submissions performed on sampling basis and, for this reason, they should be addressed considering the wider implications on the overall safety case.

| Assessment Finding Number | Assessment Finding[1] | Report Section and Technical Observation Reference[2] |
|---|---|---|
| | justification for the difference (e.g. by a PSA sensitivity analysis and a justification as to how the C&I system architecture mitigates the potential for propagation of CCF across the system).<br><br>The licensee shall ensure consistency between the reliability claims in the PSA and the C&I documentation or substantiate the basis of any difference in the figures. | TSCRep4-TO2-2.3.4-7, TSCRep4-TO2-2.4.4.1-2, TSCRep4-TO2-2.9.4.1-1, TSCRep4-TO2-2.9.4.2-1 TSCRep4-TO2-2.9.4.3-1, TSCRep3-TO2-2.2.4.3-1, TSCRep3-TO2-2.2.4.3-2 from Refs. 34, 35. |
| AF-UKABWR-CI-007 | During GDA, Hitachi-GE developed a methodology for smart device identification and justification, and applied it to candidate safety class 1 and safety class 2 devices. Whilst this approach was considered acceptable for GDA, this needs to be further developed to address the GDA scope limitations (for example, matters related to licensees' design choices) and some ONR assessment technical observations.<br><br>The Licensee shall:<br>a. Implement adequate arrangements to verify the suitability of generic smart device justifications for the site specific applications in the UK ABWR.<br>b. Complete the safety class 1 and safety class 2 justification trials, should the smart devices considered in GDA be implemented in the UK ABWR.<br>c. Extend the methodology developed for the smart device justification at safety Class 1 and safety Class 2 to safety Class 3.<br>d. Complete the development of a methodology to provide adequate level of oversight and ownership of smart device justifications contracted to 3rd parties, in accordance with the site specific intelligent customer arrangements.<br>e. Ensure that arrangements for the selection and evaluation of both the 3rd parties and internal assessors take into account the specialist software and hardware competencies required for smart device justification (e.g. commensurate with the safety class for the proposed application, the type and the complexity of the device). | Section 4.2.6 of this report |
| AF-UKABWR-CI-008 | Hitachi-GE has identified a variety of techniques and measures for the verification of the various steps in the FPGA development during GDA. ONR's expectation post GDA is that further work is carried out to identify if there are any additional measures that can be applied to the verification of the FPGA configuration (for example, using the outcome of CINIF research).<br><br>The Licensee shall undertake an options analysis exercise to determine what additional measures could be applied to confirm the correct internal configuration of the safety class 1 platform FPGA, report on the findings, and determine, so far as is reasonably practicable, if any of the identified measures should be applied. | Section 4.2.3 of this report |
| AF-UKABWR-CI-009 | During GDA Hitachi-GE provided an adequate demonstration that SSLC hardware reliability would achieve | Section 4.2.3 of this report |

[1] The assessment findings should be considered in the context defined in relevant sections of the report, which provide their justification/significance and clarify the expectation for their resolution.
[2] As clarified in Section 4.8 of the report, the TO2s should be considered as examples of observations arising from the review of Hitachi-GE submissions performed on sampling basis and, for this reason, they should be addressed considering the wider implications on the overall safety case.

| Assessment Finding Number | Assessment Finding[1] | Report Section and Technical Observation Reference[2] |
|---|---|---|
| | its targets. Post GDA ONR's expectation is that as the detailed design is developed, a full justification of key parameters (such as safe failure fraction and diagnostic coverage) is provided, taking into account, for example, the guidelines in Annex C of IEC 61508-2:2010 for SSLC modules<br><br>The Licensee shall substantiate safe failure fraction and diagnostic coverage claims for all SSLC modules, and confirm the C&I system meets reliability targets, taking into account the overall system architecture. | |
| AF-UKABWR-CI-010 | In GDA, Hitachi-GE identified a number of measures to verify the library functions/macros to be used in the safety class 1 platform. ONR's expectation is that during the detailed design an adequate justification is provided that demonstrates that risks arising from the use of library functions/macros have been reduced ALARP.<br><br>The licensee shall provide justification that pre-developed library functions/macros used in the FPGA design have been adequately verified, do not interfere with other functions, do not have unintended side effects, and do not contain unexpected functionality. | Section 4.2.3 of this report |
| AF-UKABWR-CI-011 | In GDA, Hitachi-GE established adequate principles for the testing and maintenance of the UK ABWR C&I. As further requirements are identified post GDA, ONR's expectation is that these principles are updated to reflect this.<br><br>The licensee shall:<br>a. Identify and address additional testing and maintenance requirements that arise as a result of detailed design.<br>b. Identify measures to prevent more than one division being removed from service (e.g. interlocking, procedural arrangements).<br>c. Address the consequences of testing and maintenance on reliability, and the measures necessary to manage risk.<br>d. Develop the approach to demonstrate that adequate coverage of all relevant components delivering a safety function is achieved to deliver the requirement of the safety case.<br>e. Define arrangements to support testing and maintenance and to avoid adverse interactions, such as locations, design, capability, and layout of C&I equipment. | Section 4.2.7 of this report and TSCRep2-TO2-2.1.4-3, TSCRep2-TO2-2.1.4-6, TSCRep2-TO2-2.6.4-1 in Ref. 33 and TSCRep4-TO2-2.8.4-1, TSCRep4-TO2-2.8.4-2 in Ref. 35. |
| AF-UKABWR-CI-012 | During GDA Hitachi-GE identified an adequate approach for the overall independent verification of the safety class 1 platform at module level but did not adequately address independence of verification at lower levels (e.g. at printed circuit board level). Post GDA the safety case should clarify the arrangements proposed for the verification of the safety class 1 platform at all appropriate levels.<br><br>The licensee shall review compliance against relevant standards (e.g. IEC 62566, IEC 60880) to ensure | Section 4.2.3 in this report and TSCRep3-TO2-2.2.4.2-2, TSCRep3-TO2-2.2.4.2-3, TSCRep3-TO2-2.3.4.3-1, TSCRep3-TO2-2.3.4.3-2 in Refs. 34, 35. |

[1] The assessment findings should be considered in the context defined in relevant sections of the report, which provide their justification/significance and clarify the expectation for their resolution.
[2] As clarified in Section 4.8 of the report, the TO2s should be considered as examples of observations arising from the review of Hitachi-GE submissions performed on sampling basis and, for this reason, they should be addressed considering the wider implications on the overall safety case.

| Assessment Finding Number | Assessment Finding[1] | Report Section and Technical Observation Reference[2] |
|---|---|---|
| | independent verification is performed on the safety class 1 platform at all appropriate levels, providing adequate justification that measures to detect errors will be effective in reducing risks so far as is reasonably practicable. | |
| AF-UKABWR-CI-013 | In GDA, Hitachi-GE identified a set of software tools to be used in detailed design for the development of the safety class 1 platform and application, and analysed the consequences of their failures and limitations. As the design is further developed, evidence will need to be produced on the effectiveness of the overall set of tools to detect and mitigate faults.<br><br>The licensee shall clarify:<br>a. How the measures identified to detect and mitigate tool faults have been applied.<br>b. The consequences of logic with no apparent function on simulation coverage, and the significance of this on the safety demonstration. | Section 4.2.3 in this report and TSCRep3-TO2-2.7-1, TSCRep3-TO2-2.2.4.2-5 in Ref. 34. |
| AF-UKABWR-CI-014 | During GDA Hitachi-GE provided an adequate demonstration of the suitability of the HWBS architecture and diversity requirements and have identified candidate platforms that can deliver these. ONR's assessment identified that not all system requirements may have been identified during GDA, and expects that the suitability of the site specific HWBS is substantiated when all requirements have been identified during detailed design.<br><br>The licensee shall:<br>a. Ensure that the use of setpoints for RPV water level trips is compatible with the licensee's concept of operation and is derived from the site specific fault studies, and identifies the potential need for the HWBS platform to have the capability to correct for water density changes (over all relevant temperature conditions).<br>b. Justify the suitability of the configuration of the voting arrangements, considering testing and maintenance requirements, and how the risks arising from this will be adequately managed.<br>c. Confirm and substantiate that adequate HWBS reliability can be maintained under all operational conditions, considering the number of divisions and the requirement to test and maintain equipment (including plant equipment).<br>d. Confirm the selected HWBS Human Machine Interface technology meets relevant safety case requirements, particularly in relation to the use of non-programmable components. | Section 4.2.3 in this report and TSCRep4-TO2-2.4.4.2-3 in Ref. 35. |
| AF-UKABWR-CI-015 | During GDA, Hitachi-GE provided a justification of the PCntlS meeting its performance requirement based on testing. ONR's expectation is that, once the detailed design architecture of the system is finalised, additional confirmation of the PCntlS response time will be provided.<br><br>The licensee shall confirm the performance of the PCntlS using an appropriate combination of analysis and | Section 4.2.3 in this report and TSCRep3-TO2-3.5.2-1 in Ref. 34. |

[1] The assessment findings should be considered in the context defined in relevant sections of the report, which provide their justification/significance and clarify the expectation for their resolution.
[2] As clarified in Section 4.8 of the report, the TO2s should be considered as examples of observations arising from the review of Hitachi-GE submissions performed on sampling basis and, for this reason, they should be addressed considering the wider implications on the overall safety case.

| Assessment Finding Number | Assessment Finding[1] | Report Section and Technical Observation Reference[2] |
|---|---|---|
| | testing to provide confidence that the PCntlS can achieve performance requirements under all relevant conditions. | |
| AF-UKABWR-CI-016 | The GDA C&I safety case relies for a number of functions on transfer switches (e.g. for actuator selection and transfer of command to a different control location). Although the principles for these transfer switches are acceptable, when developing its detailed design additional justifications are expected, in relation to classification, robustness and operation.<br><br>The licensee shall demonstrate the suitability of the detailed C&I design of transfer switches, to address the following:<br>a. Suitability of classification.<br>b. Failure characteristics.<br>c. Resistance to hazards (including physical and security hazards).<br>d. Human factors in operation.<br>e. Time to operate relative to timescales for fault scenarios. | Section 4.2.5 in this report and TSCRep5-TO2-2.6.4-2, TSCRep5-TO2-2.7.4-3 from Ref. 36. |
| AF-UKABWR-CI-017 | In GDA, Hitachi-GE provided outline information describing alarms. ONR's expectation is that as more detailed design information becomes available the design is adequately substantiated, in particular considering claims and engineering requirements.<br><br>The licensee shall:<br>a. Identify the engineering requirements for each alarm considering appropriate factors (such as impact on risk, aversion to alarm flood, fault detection, human factors).<br>b. justify the adequacy of the alarm design against the requirements (including the use of normally open or normally closed contacts), considering relevant good practice in the UK and relevant guidance. | Section 4.2.5 of this report and TSCRep5-TO2-2.3.4-2 from Ref. 36. |

[1] The assessment findings should be considered in the context defined in relevant sections of the report, which provide their justification/significance and clarify the expectation for their resolution.
[2] As clarified in Section 4.8 of the report, the TO2s should be considered as examples of observations arising from the review of Hitachi-GE submissions performed on sampling basis and, for this reason, they should be addressed considering the wider implications on the overall safety case.

| | | |
|---|---|---|
| AF-UKABWR-CI-018 | Whilst the principles for the C&I of the reactor building overhead crane and fuel handling machine were outlined in GDA, detailed design will depend on the licensee's choice. Based on the information available, ONR has identified a number of challenges which should be considered as part of the requirement specification and design of the systems.<br><br>The licensee shall ensure that during the detailed design of the reactor building crane, fuel handling machine, and associated equipment, that optioneering and safety analyses adequately consider all functional and non-functional requirements, including those associated with all operational and proof test requirements, to ensure that a demonstration of adequate risk control can be achieved. The optioneering and analysis to include, but not to be limited to;<br>a. Identification of all operational requirements, including those associated with non-reactor operations.<br>b. Application of the hierarchy of controls to avoid reliance on complex systems, where reasonably practicable.<br>c. The feasibility of end to end testing of all safety devices and systems (e.g. centrifugal switches).<br>d. The feasibility of qualifying components to meet safety functionality requirements and for adequate justification to be provided (e.g. complex devices such as laser scanners).<br>e. The complexity of safety measures and interactions between equipment (e.g. interlocks and vetoes to prevent collisions and enable operations). | Section 4.2.4 of this report |
| AF-UKABWR-CI-019 | In GDA, Hitachi-GE described a number of different measures to ensure that the terminal used to configure the SSLC, cannot interfere with its correct operation or introduce faults in the system. ONR's expectation as the design develops post-GDA is that evidence is provided the selected measures are shown to reduce the risk ALARP.<br><br>The licensee shall provide an ALARP demonstration to show that the risk of faults introduced by the terminal used to configure the SSLC is adequately controlled, including a demonstration that:<br>a. Connection of the terminal will not interfere with the ability of the SSLC to respond to demands.<br>b. The terminal cannot modify parameters that are not intended to be changed or it can be confirmed with sufficient integrity that other parameters have not been changed.<br>c. There is an adequate means of confirming correct parameter entry, storage and use within the SSLC. | Section 4.2.3 of this report |