Office for Nuclear Regulation

New Reactors Division – Generic Design Assessment

Step 4 Assessment of Control and Instrumentation for the UK HPR1000 Reactor

Assessment Report ONR-NR-AR-21-005
Revision 0
January 2022

Published 01/22

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

EXECUTIVE SUMMARY

This report presents the findings of my assessment of the control and instrumentation (C&I) aspects of the generic UK HPR1000 design undertaken as part of the Office for Nuclear Regulation's (ONR) Generic Design Assessment (GDA). My assessment was carried out using the Pre-Construction Safety Report (PCSR) and supporting documentation submitted by the Requesting Party (RP).

The objective of my assessment was to make a judgement, from a C&I perspective, on whether the generic UK HPR1000 design could be built and operated in Great Britain, in a way that is acceptably safe and secure (subject to site specific assessment and licensing), as an input into ONR's overall decision on whether to grant a Design Acceptance Confirmation (DAC).

The scope of my GDA assessment was to review the safety aspects of the generic UK HPR1000 design by examining the claims, arguments and supporting evidence in the safety case. My GDA Step 4 assessment built upon the work undertaken in GDA Steps 2 and 3, and enabled a judgement to be made on the adequacy of the C&I information contained within the PCSR and supporting documentation.

My assessment focussed on seeking confidence that the following aspects of the generic UK HPR1000 safety case were met from a C&I perspective:

- The safety case has been logically structured such that the 'golden thread' through claims, arguments and evidence can be clearly traced.
- The design of the C&I architecture has given due consideration to relevant good practice (RGP) and meets UK regulatory expectations.
- The platforms on which the main C&I systems of the generic UK HPR1000 design are based are suitable to support the safety requirements of the systems based on them.
- The design of the C&I systems is adequate and has followed a structured development lifecycle that is aligned with relevant good practice.
- The design of C&I platforms and systems has given due consideration to cyber-security, and the risk of a cyber-attack compromising safe operations is adequately controlled.
- Human-machine interface equipment in the main control room and remote shutdown station supports the safety functional and performance requirements of the systems that it supports.
- The RP has developed a suitable and sufficient methodology for the justification of smart devices for use in safety applications and has demonstrated that it can be practicably implemented.

The conclusions from my assessment are:

- The C&I safety case, comprising the PCSR, supporting Basis of Safety Case documents and the underpinning evidential documentation, has been adequately developed for the purposes of GDA.
- The C&I architecture is consistent with international guidance and has been adequately substantiated for the purposes of GDA.
- The RP has identified significant shortfalls in the adequacy of production excellence of the FirmSys platform against the expectations of safety Class 1 and has developed a suitable programme of work to address these shortfalls.
- The development of the hardware-based platform for the secondary protection system provides adequate diversity between different layers of defence in the C&I architecture.

- The RP has identified appropriate standards against which the centralised C&I systems will be designed and has identified compensating measures to resolve shortfalls that were revealed by compliance analysis. However, significant further work is required to complete the safety justification of the C&I platforms and systems.
- There is a lack of clarity and traceability in the specification of requirements across all C&I platforms and systems.
- From a C&I perspective I am satisfied that, given the early stage of design, the RP has given adequate consideration to the management and control of cyber-security risks.
- The HMI aspects of the C&I safety case are sufficiently well developed for the purposes of GDA.
- The RP has developed a suitable and sufficient methodology for the safety justification of smart devices and has demonstrated that this methodology can be practicably implemented.
- Noting the 24 Assessment Findings and nine minor shortfalls raised in my assessment, I am satisfied that the expectations of ONR's Safety Assessment Principles and Technical Assessment Guides are met in generic UK HPR1000 design.

These conclusions are based upon the following factors:

- A detailed and in-depth technical assessment, on a sampling basis, of the full scope of safety submissions at all hierarchy levels of the generic UK HPR1000 safety case documentation.
- Independent information, and detailed technical reviews of C&I aspects of the generic UK HPR1000 safety case undertaken for ONR by Technical Support Contractors (TSCs).
- Review of the C&I architecture and design of C&I systems and equipment against relevant ONR safety assessment principles and international standards.
- Detailed technical interactions with the RP, alongside the assessment of the responses to the substantial number of Regulatory Queries (RQs) and the Regulatory Observations (ROs) raised during the GDA.

A number of matters remain which I judge are appropriate for a licensee to consider and take forward in its site-specific safety submissions. These matters do not undermine the generic UK HPR1000 design and safety submissions but are primarily concerned with the provision of site-specific safety case evidence, which will become available as the project progresses through the detailed design, construction and commissioning stages. These matters have been captured in 24 Assessment Findings.

Overall, based on my assessment undertaken in accordance with ONR's procedures, the claims, arguments and evidence laid down within the PCSR and supporting documentation submitted as part of the GDA process present an adequate safety case for the generic UK HPR1000 design. I recommend that from a C&I perspective a DAC be granted.

LIST OF ABBREVIATIONS

ACP	Auxiliary Control Panel
AF	Assessment Finding
ALARP	As Low As Reasonably Practicable
ATWS	Anticipated Transient Without Scram
BSC	Basis of Safety Case
BSI	British Standards Institution
C&I	Control and Instrumentation
CAE	Claims-Arguments-Evidence
CBSIS	Computer-based Systems Important to Safety
CCF	Common Cause Failure
CGN	China General Nuclear Power Corporation Ltd
CIM	Component Interface Module
CINIF	Control and Instrumentation Nuclear Industry Forum
CM	Compensating Measure
COT	Core Outlet Temperature
COTS	Commercial Off The Shelf
COWP	Compact Operator WorkPlaces
CPLD	Complex Programmable Logic Device
CS&IA	Cyber Security and Information Assurance
CSDRS	Cyber Security Design Requirements Specification
CSRA	Cyber Security Risk Assessment
DAC	Design Acceptance Confirmation
DBC	Design Basis Condition
DEC	Design Extension Condition
DHP	Diverse Human-interface Panel
DiD	Defence-in-depth
ECP	Emergency Control Panel
EMI	Electromagnetic Interference
EMIT	Examination. Maintenance, Inspection and Testing
FCG3	Fangchenggang Nuclear Power Plant Unit 3
FMEA	Failure Modes and Effects Analysis
FPGA	Field Programmable Gate Array
GDA	Generic Design Assessment
GNI	General Nuclear International Ltd.
GNSL	General Nuclear System Ltd.
GSR	Generic Security Report
HCP	Hard Control Panel
HDL	Hardware Description Language

HMI	Human-Machine Interface
HOW2	(ONR) Business Management System
HPD	HDL Programmed Device
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
ICBM	Independent Confidence Building Measure
IEEE	Institute of Electrical and Electronics Engineers
IEC	International Electrotechnical Commission
ISAM	Independent Security Assurance Measure
ISO	International Organisation for Standardisation
KDS [DAS]	Diverse Actuation System
KIC [PCICS]	Plant Computer Information and Control System
KRT [PRMS]	Plant Radiation Monitoring System
LDP	Large Display Panel
MCR	Main Control Room
MDEP	Multinational Design Evaluation Programme (within OECD-NEA)
MTBF	Mean Time Between Failures
MW	Megawatts
N/A	Not Applicable
NC	Non Classified
NEA	Nuclear Energy Agency (within OECD)
NPP	Nuclear Power Plant
OECD	Organisation for Economic Cooperation and Development
ONR	Office for Nuclear Regulation
OpEx	Operational Experience
OWP	Operator Workplace
PCSR	Pre-construction Safety Report
PE	Production Excellence
pfd	Probability of Failure on Demand
PIE	Postulated Initiating Event
PSAS	Plant Standard Automation System
PSP	Protection System Panel
PWR	Pressurised Water Reactor
QA	Quality Assurance
RGL [RPICS]	Rod Position Indication and Rod Control System
RGP	Relevant Good Practice
RIC [IIS]	In-core Instrumentation System
RO	Regulatory Observation
RP	Requesting Party

RPN [NIS]	Nuclear Instrumentation System
RPS [PS]	Reactor Protection System
RSS	Remote Shutdown Station
RQ	Regulatory Query
SAP(s)	Safety Assessment Principle(s)
SAS	Safety Automation System
SCID	Safety Control and Instrumentation Device
SDM	System Design Manual
SDS	System Design Specification
SEP	Solar Energetic Particle
SFAIRP	So Far As Is Reasonably Practicable
SHP	Severe accident Human-interface Panel
SoDA	(Environment Agency's) Statement of Design Acceptability
SPM	Signal Pre-processing Module
SQEP	Suitably Qualified and Experienced Personnel
SRS	System Requirements Specification
SSC	Structures, Systems and Components
ST	Statistical Testing
SyAP(s)	Security Assessment Principle(s)
TAG	Technical Assessment Guide(s)
TO	Technical Observation (raised by the ONR TSC)
TSC	Technical Support Contractor
UK	United Kingdom
UPS	Uninterruptible Power Supply
V&V	Verification and Validation
VDU	Visual Display Unit

TABLE OF CONTENTS

Table(s)

Annex(es)

1 INTRODUCTION

1.1 Background

1. This report presents my assessment conducted as part of the Office for Nuclear Regulation (ONR) Generic Design Assessment (GDA) for the generic UK HPR1000 design within the topic of control and instrumentation (C&I).

2. The UK HPR1000 is a pressurised water reactor (PWR) design proposed for deployment in the UK. General Nuclear System Ltd (GNSL) is a UK-registered company that was established to implement the GDA on the UK HPR1000 design on behalf of three joint requesting parties (RP), i.e. China General Nuclear Power Corporation (CGN), EDF SA and General Nuclear International Ltd (GNI).

3. GDA is a process undertaken jointly by the ONR and the Environment Agency. Information on the GDA process is provided in a series of documents published on the joint regulators' website (www.onr.org.uk/new-reactors/index.htm). The outcome from the GDA process sought by the RP is a Design Acceptance Confirmation (DAC) from ONR and a Statement of Design Acceptability (SoDA) from the Environment Agency.

4. The GDA for the generic UK HPR1000 design followed a step-wise approach in a claims-argument-evidence hierarchy which commenced in 2017. Major technical interactions started in Step 2 which focussed on an examination of the main claims made by the RP for the UK HPR1000. In Step 3, the arguments which underpin those claims were examined. The Step 2 reports for individual technical areas, and the summary reports for Steps 2 and 3 are published on the joint regulators' website. The objective of Step 4 was to complete an in-depth assessment of the evidence presented by the RP to support and form the basis of the safety and security cases.

5. The full range of items that form part of my assessment is provided in ONR's GDA Guidance to Requesting Parties (Ref. 1). These include:

   - Consideration of issues identified during the earlier Step 2 and 3 assessments.
   - Judging the design against the Safety Assessment Principles (SAPs) (Ref. 2) and whether the proposed design ensures risks are As Low As Reasonably Practicable (ALARP).
   - Reviewing details of the RP's design controls and quality control arrangements to secure compliance with the design intent.
   - Establishing whether the system performance, safety classification, and reliability requirements are substantiated by a more detailed engineering design.
   - Assessing arrangements for ensuring and assuring that safety claims and assumptions will be realised in the final as-built design.
   - Resolution of identified nuclear safety and security issues, or else identifying paths for resolution.

6. The purpose of this report is therefore to summarise my assessment in the C&I topic which provides an input to the ONR decision on whether to grant a DAC, or otherwise. This assessment was focused on the submissions made by the RP throughout GDA, including those provided in response to the Regulatory Queries (RQs) and Regulatory Observations (ROs) I raised. Any ROs issued to the RP are published on the GDA's joint regulators' website, together with the corresponding resolution plans.

1.2 Scope of this Report

7. This report presents the findings of my assessment of the C&I aspects of the generic UK HPR1000 design undertaken as part of GDA. I carried out my assessment on the

Pre-construction Safety Report (PCSR) (Ref. 3) and supporting documentation submitted by the RP. My assessment was focussed on considering whether the generic UK HPR1000 safety case provides an adequate justification for the generic UK HPR1000 design, in line with the objectives for GDA.

1.3 Methodology

8. The methodology for my assessment follows ONR's guidance on the mechanics of assessment, NS-TAST-GD-096 (Ref. 4).

9. My assessment was undertaken in accordance with the requirements of ONR's How2 Business Management System (BMS). ONR's SAPs (Ref. 2) and Security Assessment Principles (SyAPs) (Ref. 5), together with supporting Technical Assessment Guides (TAGs) (Ref. 6), were used as the basis for my assessment. Further details are provided in Section 2. Note, assessment against the SyAPs (Ref. 5) has been performed collaboratively with a CS&IA inspector and is documented in an assessment note (Ref. 7); I have taken the outcomes of this assessment into account. The outputs from my assessment are consistent with ONR's GDA guidance to RPs (Ref. 1).

2 ASSESSMENT STRATEGY

10. The strategy for my assessment of the C&I aspects of the generic UK HPR1000 design and safety case is set out in this section. This identifies the scope of the assessment and the standards and criteria that have been applied.

2.1 Assessment Scope

11. A detailed description of my approach to this assessment can be found in assessment plan ONR-GDA-UKHPR1000-AP-19-004. Rev 0 (Ref. 8).

12. I considered all of the main submissions within the remit of my assessment scope, to various degrees of breadth and depth. I chose to concentrate my assessment on those aspects of the C&I design that I judged to have the greatest safety significance, or where the hazards appeared least well controlled. My assessment was also influenced by the claims made by the RP, my previous experience of similar systems for reactors and other nuclear facilities, and any identified gaps in the original submissions made by the RP. A particular focus of my assessment has been the ROs and RQs I raised as a result of my on-going assessment, and the resolution thereof.

2.2 Sampling Strategy

13. In line with ONR's guidance (Ref. 4) and as detailed in my assessment plan (Ref. 8), I chose a sample of the RP's submissions to undertake my assessment. The main themes considered are summarised below:

- Structure and clarity of safety case – I sought to understand the 'golden thread' through claims, arguments and evidence and a demonstration of how relevant good practice has been addressed in the safety case.

- Adequacy of the C&I architecture – I considered the design of the C&I architecture against relevant good practice (RGP) with particular regard to the following:

  - the provision of defence-in-depth (DiD) to protect against design basis faults and design extension conditions;
  - independence between systems, and between redundant parts of the same system, to provide resilience against common cause failure (CCF) and protection against failure propagation; and
  - measures to prevent the spurious actuation of C&I systems leading to significant consequences.

- Adequacy of C&I platforms – I have assessed the platforms on which the centralised C&I systems of the generic UK HPR1000 design are based, and in particular their suitability to support the safety requirements of the systems based on them.

- Adequacy of C&I systems – I have assessed the design of the UK HPR1000 centralised C&I systems. Specifically the reactor protection system (RPS [PS]), safety automation system (SAS), diverse actuation system (KDS [DAS]), plant standard automation system (PSAS), plant computer information and control system (KIC [PCICS]), and severe accident system (KDA [SA I&C]).My assessment sought confidence in the following:

  - the extent to which the safety functional and performance requirements for C&I systems have been informed by the UK HPR1000 fault analysis;

- demonstration of how the development processes applied by the RP ensure that system requirements are fulfilled, including compliance with codes and standards applicable to the development;
- a demonstration of production excellence (PE) and the strategy for conducting independent confidence building measures (ICBM) for the main computer-based C&I systems and equipment;
- requirements for the design of non-centralised C&I systems and equipment important to safety; and
- requirements for examination, maintenance, inspection and testing (EMIT) of C&I systems and how these have been derived in the safety case.

- Adequacy of human-machine interfaces (HMI) – I have assessed the design scheme for HMI equipment in the main control room (MCR) and remote shutdown station (RSS) to understand how it supports the safety functional and performance requirements and how RGP has been considered in the design.

- Cyber security of C&I systems important to safety – I collaborated with the ONR cyber security and information assurance (CS&IA) specialist to assess the RP's cyber security risk assessments for the centralised C&I systems and equipment. I also sought evidence of the extent to which security has been taken into account in the development of C&I platforms and systems, and the strategy for independent cyber security assurance of C&I systems.

- Approach to justification of smart devices for use in safety applications – I sought confidence in the RP's ability to meet UK regulatory expectations in this area through assessment of its justification methodology and sample device justifications.

2.3 Out of Scope Items

14. The following items were outside the scope of my assessment.

- My assessment of non-centralised C&I systems was limited to consideration of high-level requirements (e.g. safety functions, system classification and interfaces to centralised C&I systems). Detailed design and equipment selection will be undertaken post-GDA hence these elements were outside the scope of my assessment.

2.4 Standards and Criteria

15. The relevant standards and criteria adopted within this assessment are principally the SAPs (Ref. 2), SyAPs (Ref. 5), TAGs (Ref. 6), relevant national and international standards, and relevant good practice informed from existing practices adopted on nuclear licensed sites in Great Britain. The key SAPs and any relevant TAGs, national and international standards and guidance are detailed within this section. RGP, where applicable, is cited within the body of the assessment.

2.4.1 Safety and Security Assessment Principles

16. The SAPs (Ref. 2) and SyAPs (Ref. 5) constitute the regulatory principles against which ONR judge the adequacy of safety and security cases. The SAPs and SyAPs applicable to C&I are included within Annex 1 of this report.

17. The key SAPs applied within my assessment include SAPs ECS.1, ECS.2, ECS.3, EDR.1, EDR.2, EDR.3, EDR,4, ERL.1, ERL.2 and the safety system SAPs ESS.1 –

ESS.27. Additionally, my assessment of the cyber security of C&I systems has considered SyAP FSyp7.

2.4.2 Technical Assessment Guides

18. The following Technical Assessment Guides were used as part of this assessment:

- NS-TAST-GD-003, *Safety Systems* (Ref. 9)*;*
- NS-TAST-GD-046, *Computer Based Safety Systems* (Ref. 10)*;*
- NS-TAST-GD-005, *ONR Guidance on the Demonstration of ALARP* (Ref. 11)*;*
- NS-TAST-GD-051, *The Purpose, Scope and Content of Nuclear Safety Cases* (Ref. 12)*;* and
- NS-TAST-GD-094, *Categorisation of Safety Functions and Classification of Structures, Systems and Components* (Ref. 13)*.*

2.4.3 National and International Standards and Guidance

19. The standards considered as part of my assessment are listed below. The RP's identification and application of relevant standards and guidance to the C&I design and safety case is discussed in the detailed technical assessment in Section 4 of this report.

- BS EN IEC 60709, *Nuclear power plants. Instrumentation, control and electrical systems important to safety. Separation* (Ref. 14);
- BS EN 60780, *Nuclear facilities. Electrical equipment important to safety. Qualification* (Ref. 15);
- BS EN 60880, *Nuclear power plants. Instrumentation and control systems important to safety. Software aspects for computer-based systems performing category A functions* (Ref. 16);
- BS EN 60987, *Nuclear power plants. Instrumentation and control important to safety. Hardware design requirements for computer-based systems* (Ref. 17);
- BS EN IEC 61226, *Nuclear power plants. Instrumentation, control and electrical power systems important to safety. Categorization of functions and classification of systems* (Ref. 18);
- BS EN IEC 61500, *Nuclear power plants. Instrumentation and control systems important to safety. Data communication in systems performing category A functions* (Ref. 19);
- BS EN IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems* (Ref. 20);
- BS IEC 61513, *Nuclear power plants. Instrumentation and control important to safety. General requirements for systems* (Ref. 21);
- BS EN IEC 62138, *Nuclear power plants. Instrumentation and control systems important to safety. Software aspects for computer-based systems performing category B or C functions* (Ref. 22);
- BS EN 62340, *Nuclear power plants. Instrumentation and control systems important to safety. Requirements for coping with common cause failure* (Ref. 23);
- BS EN 62566, *Nuclear power plants. Instrumentation and control important to safety. Development of HDL-programmed integrated circuits for systems performing category A functions* (Ref. 24);
- BS EN IEC 62566 part 2, *Nuclear power plants. Instrumentation and control systems important to safety. Development of HDL-programmed integrated circuits. HDL-programmed integrated circuits for systems performing category B or C functions* (Ref. 25);
- BS EN IEC 62645, *Nuclear power plants. Instrumentation, control and electrical power systems. Cybersecurity requirements* (Ref. 26);
- BS EN IEC 62859, *Nuclear power plants. Instrumentation and control systems. Requirements for coordinating safety and cybersecurity* (Ref. 27);

- ISO/IEC 27005, *Information technology. Security techniques. Information security risk management* (Ref. 28);
- IAEA SSG-30, *Safety Classification of Structures, Systems and Components in Nuclear Power Plants* (Ref. 29); and
- IAEA SSG-39, *Design of Instrumentation and Control Systems for Nuclear Power Plants* (Ref. 30).

2.5 Use of Technical Support Contractors

20. It is usual in GDA for ONR to use Technical Support Contractors (TSCs) to provide access to independent advice and experience, analysis techniques and models, and to enable ONR's inspectors to focus on regulatory decision making.

21. Table 1 below sets out the areas in which I used TSCs to support my assessment. I required this support to provide additional capacity for the review of technical documentation and to access independent advice and experience. The scope of work undertaken by the ONR TSC included:

- Reviews of evidence provided to answer Technical Observations (TOs) raised by previous TSC reviews during Step 3, and documented in reports (Ref. 31), (Ref. 32) and (Ref. 33).
- Independent technical reviews of the submissions provided by the RP against ONR's regulatory expectations as defined in the SAPs, SyAPs and TAGs, as well as the relevant standards and guidance listed above.
- Supporting ONR in the raising of RQs to address gaps in submissions, review of the RP's responses and provision of advice to ONR on the adequacy of those responses.
- Identification of areas where additional work was required to address shortfalls in the RP's safety case and supporting ONR in raising ROs to identify actions required for resolution.
- Support to ONR at meetings with the RP to facilitate effective and efficient exchange of information, and to allow the ONR TSC to ask specific technical questions of the RP's subject matter experts. ONR was present at all interactions between the RP and the ONR TSC.

Table 1: Work Packages Undertaken by the ONR TSC

Number	Description
1	Structure and Clarity of C&I Safety Case (Ref. 34)
2	Evidence of Adequacy of C&I Architecture (Ref. 35)
3	Cyber Security (Ref. 36)
4	Confirmation of Adequacy of the Platforms (Ref. 37)
5	Confirmation of the Adequacy of the Systems (Ref. 38)
6	Confirmation of the Adequacy of the Human-machine Interface (Ref. 39)

22. Whilst the ONR TSC undertook detailed technical reviews, this was done under my direction and close supervision. The regulatory judgment on the adequacy, or otherwise, of the generic UK HPR1000 safety and security case in this report has been made exclusively by ONR inspectors.

2.6 Integration with Other Assessment Topics

23. GDA requires the submission of an adequate, coherent and holistic generic UK HPR1000 safety case. Regulatory assessment cannot be carried out in isolation as there are often issues that span multiple disciplines. I have therefore worked closely with a number of other ONR inspectors to inform my assessment. The key interactions were:

- I worked with the ONR Fault Studies specialist inspector in my assessments of the analysis of the consequences of spurious C&I actuation, and the diversity and independence of C&I systems.
- I consulted with specialists from Fault Studies and Mechanical Engineering in my assessment of the C&I architecture, in particular regarding the sharing of field equipment.
- I worked closely with the ONR cyber security and information assurance (CS&IA) specialist inspector in my assessment of the cyber security of C&I systems.
- I worked with specialists from Fault Studies, Electrical Engineering and Mechanical Engineering to assess the RP's response to RO-UKHPR1000-0021 'Demonstration of the adequacy of Examination, Maintenance, Inspection and Testing (EMIT) of structures, systems and components important to safety' (Ref. 40) regarding the requirements for EMIT of structures, systems and components (SSCs).
- I consulted with specialists from Fault Studies, Electrical Engineering, Mechanical Engineering and severe accident analysis in my assessment of the adequacy of C&I systems, in particular regarding categorisation of safety functions, classification of systems, and derivation of requirements from the safety analysis.
- I consulted with ONR specialist inspectors from Internal and External Hazards in my assessment of the adequacy of the C&I architecture, in particular regarding the resilience of the C&I architecture to internal and external hazards.
- I engaged with the ONR Human Factors specialist inspector in my assessment of the suitability of human-machine interfaces to gain confidence that the approach appropriately considers the human factors requirements.
- I liaised with the ONR Electrical Engineering specialist inspector in my assessment of the smart device substantiation methodology to ensure that the methodology was suitable for electrical smart devices.
- I worked with ONR specialists from Electrical Engineering, Mechanical Engineering and Fault Studies on the assessment of RO-UKHPR1000-0039 'Performance Analysis of UK HPR1000 Heating Ventilation and Air Conditioning Systems' (Ref. 40). My contribution to this assessment is documented in an assessment note (Ref. 41).
- I worked with the ONR Probabilistic Safety Assessment specialist on the assessment of RO-UKHPR1000-0013 'Modelling of Computer-Based System Reliability in the PSA' (Ref. 40). My contribution to this assessment is documented in an assessment note (Ref. 42).

- I worked with ONR specialists from Mechanical Engineering, Fault Studies and fuel and core on the assessment of RO-UKHPR1000-0056 ‘Fuel Route Safety Case’ (Ref. 40). My contribution to this assessment is documented in an assessment note (Ref. 43).

3 REQUESTING PARTY'S SAFETY CASE

3.1 Introduction to the Generic UK HPR1000 Design

24. The generic UK HPR1000 design is described in detail in the PCSR (Ref. 3). It is a three-loop PWR designed by CGN using Chinese Hualong technology. The generic UK HPR1000 design has evolved from reactors which have been constructed and operated in China since the late 1980s, including the M310 design used at Daya Bay and Ling'ao (Units 1 and 2), the CPR1000, the CPR1000^{+} and the more recent ACPR1000. The first two units of CGN's HPR1000, Fangchenggang Nuclear Power Plant (NPP) Units 3 and 4, are under construction in China and Unit 3 is the reference plant for the generic UK HPR1000 design. The design is claimed to have a lifetime of at least 60 years and has a nominal electrical output of 1,180 MW.

25. The reactor core contains zirconium clad uranium dioxide (UO_2) fuel assemblies and reactivity is controlled by a combination of control rods, soluble boron in the coolant and burnable poisons within the fuel. The core is contained within a steel Reactor Pressure Vessel which is connected to the key primary circuit components, including the Reactor Coolant Pumps, Steam Generators, pressuriser and associated piping, in the three-loop configuration. The design also includes a number of auxiliary systems that allow normal operation of the plant, as well as active and passive safety systems to provide protection in the case of faults, all contained within a number of dedicated buildings.

26. The reactor building houses the reactor and primary circuit and is based on a double-walled containment with a large free volume. Three separate safeguard buildings surround the reactor building and house key safety systems and the main control room. The fuel building is also adjacent to the reactor and contains the fuel handling and short-term storage facilities. Finally, the nuclear auxiliary building contains a number of systems that support operation of the reactor. In combination with the diesel, personnel access and equipment access buildings, these constitute the nuclear island for the generic UK HPR1000 design.

27. The main systems that comprise the UK HPR1000 C&I architecture are described in detail in Chapter 8 of the PCSR (Ref. 3) and are summarised below:

- Class 1 RPS [PS] is the primary protection system, performing Category A safety functions to bring the plant to a controlled state in the event of a fault. The RPS [PS] is based on the FirmSys platform.
- Class 2 SAS performs Category B safety functions to bring the plant from the controlled state to a safe shutdown state. The SAS is also based on the FirmSys platform.
- Class 2 KDS [DAS] performs Category B safety functions to bring the plant to a safe state in the event of a frequent fault concurrent with failure of the RPS [PS] and the SAS. The KDS [DAS] is based on a simple hardware-based platform which is being newly engineered for the UK HPR1000 project.
- Class 3 PSAS and KIC [PCICS] provide control and monitoring of the plant during normal operation. Both the PSAS and KIC [PCICS] are based on the HOLLiAS-N platform.
- Class 3 KDA [SA I&C] provides control and monitoring functions during severe accidents and is based on the SpeedyHold platform.

28. The FirmSys, HOLLiAS-N and SpeedyHold platforms on which the RPS [PS], SAS, PSAS, KIC [PCICS] and KDA [SA I&C] are respectively based are pre-existing platforms that are provided by third party suppliers and as such can be considered as commercial off-the-shelf (COTS) equipment.

29. The centralised systems listed above interface with non-centralised systems for the control and monitoring of specific plant items. The non-centralised C&I systems are described in the PCSR (Ref. 3). Given the scope of my assessment of the non-centralised C&I systems described in paragraph 14, only limited sampling of these systems was performed. Those non-centralised systems that were pertinent to my assessment included:

- Nuclear Instrumentation System (RPN [NIS]).
- Plant Radiation Monitoring System (KRT [PRMS]).
- In-core Instrumentation System (RIC [IIS]).
- Rod Position Indication and Rod Control System (RGL [RPICS]).

3.2 The Generic UK HPR1000 Safety Case.

30. In this section I provide an overview of the C&I aspects of the generic UK HPR1000 safety case as provided by the RP during GDA. Details of the technical content of the documentation and my assessment of its adequacy are reported in the subsequent sections of my report.

31. The UK HPR1000 C&I safety case uses a claims, arguments and evidence (CAE) structure. In order to present a clear and logical case it is separated into three ‘tiers’. The top-tier document is Chapter 8 of the PCSR (Ref. 3) which sets out the high-level claims and arguments for the C&I design.

32. Tier two comprises a series of basis of safety case (BSC) documents, each of which addresses a separate aspect of the C&I design as follows:

- Overall C&I Architecture (Ref. 44)
- RPS [PS] (Ref. 45)
- SAS (Ref. 46)
- KDS [DAS] (Ref. 47)
- PSAS (Ref. 48)
- KIC [PCICS] (Ref. 49)
- KDA [SA I&C] (Ref. 50)

33. The BSCs further decompose the high-level claims from the PCSR into specific sub-claims and arguments. The C&I architecture BSC sets out the claims, subclaims and arguments associated with the C&I architecture design and provides links to the evidence underpinning the arguments. The individual system level BSCs provide the same CAE structure and identify the safety functional and safety feature claims for each C&I system.

34. Tier 2 also includes topic reports for each of the platforms on which the computer-based C&I systems are based (Ref. 51), (Ref. 52) and (Ref. 53). These topic reports provide detailed descriptions of the architecture, functionality, development and qualification processes of each platform.

35. Tier 3 consists of the engineering design and justification documents for the C&I architecture and systems, which provides the evidence supporting the claims and arguments.

36. The principal evidential documents supporting the justification of the C&I architecture include an architecture design specification (Ref. 54), analyses of the independence (Ref. 55) and diversity (Ref. 56) between systems, and a study of the reliability of the centralised C&I systems (Ref. 57).

37. The RP provided documents relating to both the design development and safety justification of the centralised C&I systems important to safety. These include the following:

- System requirements specifications (SRS) for each system – (Ref. 58), (Ref. 59), (Ref. 60), (Ref. 61), (Ref. 62) and (Ref. 63) (Ref. 64).
- System design specifications (SDS) for each system – (Ref. 65), (Ref. 66), (Ref. 67) (Ref. 68), (Ref. 69) and (Ref. 70).
- Documents demonstrating the production excellence (PE) of computer-based platforms and systems – (Ref. 71), (Ref. 72), (Ref. 73) , (Ref. 74) , (Ref. 75), (Ref. 76) , (Ref. 77), (Ref. 78).
- Documents setting out the strategy for conducting independent confidence building measures for computer-based systems – (Ref. 79), (Ref. 80), (Ref. 81) and (Ref. 82).
- Standards compliance analyses for the C&I platforms – (Ref. 83), (Ref. 84), (Ref. 85) and (Ref. 86).
- Standards compliance analyses for the C&I systems – (Ref. 87), (Ref. 88), (Ref. 89), (Ref. 90), (Ref. 91), (Ref. 92), (Ref. 93), (Ref. 94) and (Ref. 95).
- Failure modes and effects analyses (FMEA) of the platforms for the main protection systems – (Ref. 96), (Ref. 97) and (Ref. 98).

38. Figure 1 gives a representation of the structure of the C&I safety case and the relationship between the top-level submissions and the supporting documentation.

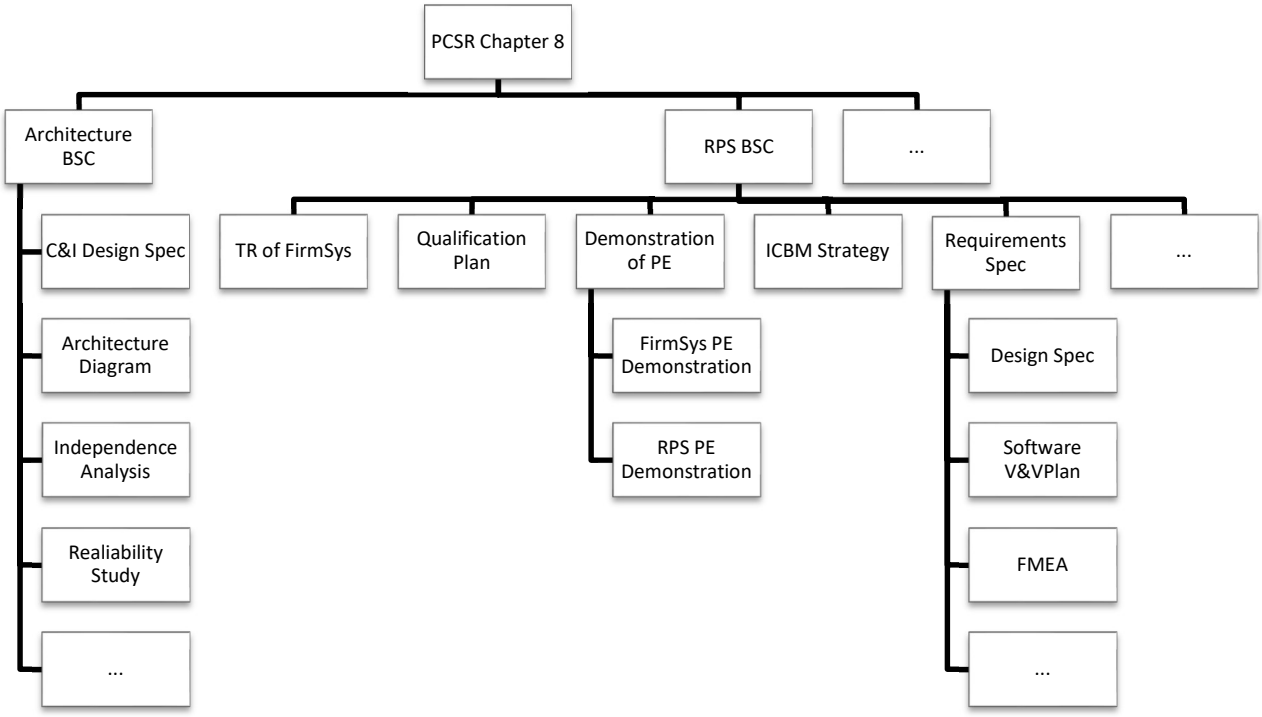

Figure 1: Example document map of the UK HPR100 C&I safety case

4 ONR ASSESSMENT

4.1 Structure of Assessment Undertaken

39. The following sub-sections detail the assessment I have undertaken during GDA Step 4. The assessment is structured around the sampling strategy outlined in paragraph 13 and covers the following technical topic areas:

- 41 Safety Case Structure and Clarity
- 4.3 Adequacy of C&I Architecture
- 175 Examination, Maintenance, Inspection and Testing (EMIT) of C&I systems
- 4.5 Adequacy of C&I Platforms
  - 195 Adequacy of the FirmSys Platform
  - 218 Adequacy of the Simple Hardware Platform
  - 4.5.3 Adequacy of the HOLLiAS-N Platform
  - 4.5.4 Adequacy of the SpeedyHold Platform
- 271 Adequacy of C&I Systems
  - 4.6.1 Adequacy of the RPS [PS]
  - 4.6.2 Adequacy of the SAS
  - 4.6.3 Adequacy of the KDS [DAS]
  - 4.6.4 Adequacy of the PSAS
  - 408 Adequacy of the KIC [PCICS]
  - 427 Adequacy of the KDA [SA I&C]
- 4.7 Independent Confidence Building Measures for all Systems
- 4.8 Cyber Security of C&I Systems
- 500 Adequacy of HMI
- 546 Justification of Smart Devices
- 4.11 Demonstration that Relevant Risks Have Been Reduced to ALARP
- 4.12 Consolidated Safety Case (Chapter 8)
- 4.13 Comparison with Standards, Guidance and Relevant Good Practice

40. A number of regulatory observations (ROs) related to aspects of the C&I design were raised in earlier steps of GDA, including the adequacy of the diverse actuation system, the independence in the C&I architecture and the demonstration of compliance with RGP. My assessment has covered these ROs.

41. My assessment has focused on confirming that the safety case, design principles and the design lifecycle of C&I systems important to safety meet ONR's regulatory expectations and that there is adequate evidence that these have been demonstrably applied to the generic C&I design.

4.2 Safety Case Structure and Clarity

4.2.1 Assessment

42. I sought to establish confidence in the structure of the RP's safety case through understanding the key claims related to C&I, how these are traced through the case and underpinned by supporting evidence. I also wanted to understand how the C&I design has considered RGP such as that defined in international standards. The key SAPs (Ref. 2) that informed this aspect of my assessment included SC.1, SC.4, including the guidance in NS-TAST-GD-051 (Ref. 12), ECS.3 and ECS.5. In undertaking my assessment I sampled relevant submissions, including:

- PCSR Chapter 8 (Revision 2) (Ref. 3).
- 'BSC of Overall I&C Architecture' (Revision F) (Ref. 44).
- 'BSC of Protection System' (Revision F) (Ref. 99).
- 'BSC of Safety Automation System' (Revision C) (Ref. 100).
- 'BSC of Diverse Actuation System' (Revision C) (Ref. 101).
- 'BSC of Plant Standard Automation' (Revision C) System (Ref. 48).
- 'BSC of Plant Computer Information and Control System' (Revision D) (Ref. 49).
- 'BSC of Severe Accident I&C System' (Revision C) (Ref. 102).
- 'ALARP Demonstration Report of PCSR Chapter 8' (Revision F) (Ref. 103).
- 'Suitability Analysis of Codes and Standards in I&C Topic Area' (Revision C) (Ref. 104).
- 'Production Strategy for Instrumentation and Control' (Revision F) (Ref. 105).
- 'SAS System Requirements Specification' (Revision D) (Ref. 106).
- 'PSAS System Requirements Specification' (Revision D) (Ref. 61).

43. The RP provided a 'production strategy' (Ref. 105) which set out the document structure of the C&I safety case and described how the 'golden thread' would be developed. As described in Section 3.2 the C&I safety case is described in a structured set of documents, with Chapter 8 of the PCSR (Ref. 3) being the top-level document and a series of BSCs and lower level documents providing the claims, arguments and evidence.

44. In my assessment I have considered the expectations of NS-TAST-GD-051 (Ref. 12) and the extent to which the safety case meets the following criteria:

- intelligible – understandable and accessible to meet the needs of its users;
- valid – accurately represents the status of the design;
- complete – all activities and modes of operation are analysed;
- evidential – claims and arguments are supported by verifiable evidence;
- robust – the case conforms to relevant good practice;
- integrated – interactions and dependencies with other areas are identified;
- balanced – a balanced view of risk, uncertainty, weaknesses and improvements is provided; and
- forward looking – considers safe operation for the plant's defined lifetime.

45. In GDA Step 2 ONR found that there were no clear links between C&I and other areas of the safety case, and that the CAE structure did not meet ONR's regulatory expectations. This was addressed at the start of Step 3 where a revised C&I claims structure was presented in a revision to Chapter 8 of the PCSR (Ref. 107) along with the supporting arguments in the form of the BSCs. My assessment of Revision B of the 'BSC of Overall I&C Architecture' (Ref. 108) found that there was insufficient detail presented in the arguments to demonstrate how the claims would be met.

46. I therefore raised RQ-UKHPR1000-0176 (Ref. 109) requesting clarification on how the safety case would be further developed to provide greater visibility of the 'golden thread'. In addition, since the ONR Electrical Engineering inspector had identified similar issues with the electrical safety case, we delivered a joint presentation to the RP to set out our concerns and expectations at a workshop early in Step 3 (Ref. 110).

47. The RP subsequently provided Revision C of the C&I architecture BSC (Ref. 111) as well as BSCs for the C&I systems. I sampled the architecture BSC as well as Revision B of the BSC for the RPS [PS] (Ref. 112) and Revision of the KDS [DAS] BSC (Ref. 113) and found that, while my concerns had been partially addressed, there remained significant shortfalls in the completeness and consistency of the C&I safety case, and in particular the arguments did not adequately describe how the evidence supported the claims.

48. An example of this was claim C.2.1.1 in the RPS [PS] BSC (Ref. 112), which stated "The reliability design of the RPS [PS] is commensurate with their safety significance." The argument provided in support of this claim merely stated that the claim was met, rather than explaining how the evidence cited (i.e. FMEA of Protection System (Ref. 114) and the Independence Analysis of I&C Systems (Ref. 115)) demonstrates this. I was not satisfied that the expectations of NS-TAST-GD-051 (Ref. 12) were met, with particular regard to intelligibility, validity, completeness, evidentiality and robustness.

49. My expectation for Step 4 was therefore that the RP would further develop the safety case to address these shortfalls and demonstrate that the C&I claims are satisfied by the arguments and evidence provided.

50. To enable the RP to understand ONR's regulatory expectations I arranged a workshop early in Step 4 (Ref. 116) where we further discussed the approach to CAE and explored the shortfalls in the C&I safety case. Following this the RP submitted further revisions of each of the BSCs – (Ref. 117), (Ref. 118), (Ref. 119), (Ref. 120), (Ref. 121), (Ref. 122) and (Ref. 123). To assess whether my expectations regarding the structure of the case had been met I conducted a sample review of the documents for the C&I architecture (Ref. 117) and the RPS [PS] (Ref. 118), and found that the RP had made significant improvements in the CAE structure. In particular I noted the following:

- claims and sub-claims had been further broken down such that each argument addresses one specific point;
- arguments provided a summary of how the C&I design has been developed to address the claims, and provide links to the detailed underpinning evidence; and
- explicit references we provided to the specific section(s) in evidential documents that supported the argument.

51. Through my review I identified some inconsistencies in the referencing of evidence, in particular several instances where superseded versions of documents were referenced. I therefore raised RQ-UKHPR1000-1573 (Ref. 109) asking the RP to explain how these inconsistencies would be addressed. In response the RP undertook a review of all BSC documents, cross-checking the referenced evidence, which identified similar inconsistencies throughout the safety case. These inconsistencies have been corrected in the latest revisions of the BSCs (Ref. 44), (Ref. 45) (Ref. 46), (Ref. 47), (Ref. 48), (Ref. 49) and (Ref. 50).

52. My assessment of the structure of the C&I safety case found that the rationale is sufficiently clear, it is possible to trace the 'golden thread' through the documentation, and the CAE structure is adequately developed for this stage of the project. I was satisfied that the RP had followed the approach outlined in the production strategy (Ref. 105) and that the expectations of NS-TAST-GD-051 (Ref. 12) for the structure of safety cases were broadly met.

53. The ONR TSC raised a number of technical observations in its reports (Ref. 34) – (Ref. 38) relating to inconsistencies within the safety case. While these were not significant enough to impact my ability to complete a meaningful assessment, my expectation is that the inconsistencies will be resolved by the licensee as the safety case evolves. I have therefore raised this as part of AF-UKHPR1000-0052 (see Section 4.11).

54. During Step 3 I identified potential regulatory shortfalls associated with the demonstration of how RGP has been considered in the C&I design, particularly with regard to how normative and informative requirements of RGP are addressed. I therefore raised RO-UKHPR1000-0016 'Demonstration of compliance with relevant good practice for control and instrumentation' (Ref. 40), to:

- explain ONR's regulatory expectations for the identification of and demonstration of compliance with RGP;
- ensure the RP adequately identifies all RGP it considers applicable to the UK HPR1000 C&I design, and that a suitable and sufficient justification of compliance with that RGP is provided in the UK HPR1000 C&I safety case;
- ensure that all relevant evidence, including information from the Fangchenggang NPP Unit 3 (FCG3) design is appropriately identified and provided in the UK HPR1000 safety case; and
- obtain confidence that shortfalls against C&I RGP are identified and suitably addressed in the generic UK HPR1000 design, thereby supporting a robust ALARP case.

55. My detailed assessment of the response to this RO is documented in an assessment note (Ref. 124) and is not repeated in full here. However, the key points are summarised in the below paragraphs.

56. The 'ALARP demonstration report of PCSR Chapter 8' (Ref. 103) identifies codes and standards that have been considered in the reference design. The applicability of these codes and standards is justified in a separate document (Ref. 104). I reviewed these submissions and found that the RP had identified 82 codes and standards from various sources, including Chinese nuclear regulations and standards, IAEA standards, IEC standards and IEEE standards. To select those standards applicable to the UK HPR1000 C&I design a screening process was applied which resulted in 34 standards being identified as applicable. For these 34 standards an analysis is presented to justify the relevance of the standard, the scope of its applicability to the design and discussion on the impact of the standard on the reference design.

57. Based on my review of the documentation I was content that the codes and standards applied to the UK HPR1000 C&I design are appropriate and that the RP had provided suitable justifications for the applicability of those codes and standards, as well as for the non-application of standards screened out by its review (for example, several Chinese and IEEE standards are screened out because alternative standards exist that are identified in ONR's TAGs as relevant good practice).

58. I reviewed the 'BSC of Protection System' (Ref. 99) and found that it included numerous claims relating to compliance with RGP including national and international standards. My review identified that some standards appeared not to have been considered. I therefore raised RQ-UKHPR1000-1010 (Ref. 109) seeking clarification on these apparent omissions. In response the RP stated that these standards are considered at the architectural level and are therefore addressed in the 'BSC of Overall I&C Architecture' (Ref. 44). I reviewed that document and was content that the standards had been adequately considered. I judge the failure to specifically address these standards at the system level to be a minor shortfall.

59. The 'ALARP demonstration report of PCSR Chapter 8' (Ref. 103) also includes an analysis of operational experience, including information from the reference plant design (FCG3), on which the UK HPR1000 C&I design is based. The relevant evidence has been incorporated into the 'golden thread' within the BSCs; this is most relevant to the RPS [PS] as the functional requirements and control logic are very similar between the generic UK HPR1000 design and the reference plant (FCG3). In order to trace the 'golden thread' and understand how evidence from the reference plant supports the C&I claims, I sampled the Revision F of the 'BSC of Protection System' (Ref. 99) and supporting documentation. I identified several instances where evidence from the reference plant was cited as underpinning the claims and arguments; for example in the 'Demonstration of Production Excellence for FirmSys Platform' (Ref. 71). I sampled some of this evidence, relating to equipment qualification testing, (Ref. 125) and was content that it corroborated the claims within the safety

case. The detailed assessment of production excellence of the C&I platforms is documented in Section 4.5 of this report.

60. My review of the BSC for the RPS [PS] identified that some claims, particularly relating to environmental qualification of the system, did not refer to evidence from the reference plant, even though such evidence is referenced elsewhere in the safety case and it should be considered relevant to the claim. I consider this inconsistency in the safety case to be a minor shortfall in compliance with SAP ECS.5 (Ref. 2).

61. The 'ALARP Demonstration Report of PCSR Chapter 8' (Ref. 103) provides a list of gaps that have been identified through the RP's comparison of the UKHPR1000 C&I design with RGP. Against each gap I noted that the RP had provided a justification as to how it had been addressed within GDA, along with a brief summary of the associated optioneering that had been performed – with references provided to documents that describe the optioneering in greater detail. I sampled one such document, relating to a modification to introduce additional diversity in fault detection for some reactor protection functions (Ref. 126). My review found that the scope of the modification was clearly defined, that the optioneering was well described and that a suitable justification was provided for the selected option.

62. Having assessed the submissions provided in response to RO-UKHPR1000-0016 I was content that the RP had adequately identified the RGP applicable to the UK HPR1000 C&I design and had provided a suitable and sufficient demonstration of compliance. I was content that the RP had met the intent of RO and on this basis the RO was closed (Ref. 124).

63. An important aspect of justification of the suitability of the C&I design is demonstration that it adequately addresses the requirements of international standards that are considered RGP in the UK nuclear industry (for example the IEC SC 45A series). In this regard the RP undertook analyses demonstrating how the design of the C&I platforms (Ref. 83) – (Ref. 87) and systems (Ref. 88) – (Ref. 95) comply with the key standards that inform ONR's regulatory expectations.

64. I sampled these documents, focussing on those relating to the systems of highest safety significance, i.e. the FirmSys platform and the RPS [PS] and SAS. My review identified that in several cases the compliance statements were assertions that particular clauses had been met, without any argumentation or references to evidence that underpins the claim. I therefore raised a series of RQs (RQ-UKHPR1000-1000, 1116, 1354, 1355 and 1360) (Ref. 109) seeking additional justification of compliance.

65. For the FirmSys platform the RP undertook further standards compliance analyses as part of the response to RO-UKHPR1000-0059 'Evidence of Production Excellence for the FirmSys platform' (Ref. 40); this is assessed in detail in sub-section 195 of this report and is not discussed further here. For the RPS [PS] and SAS, while the responses to RQ-UKHPR1000-1354, 1355 and 1360 (Ref. 109) provided some clarification, several queries were not fully resolved. In the responses to these RQs the RP committed to undertaking further standards compliance analyses for the C&I systems during the detailed design and substantiation of the systems.

66. I was satisfied that the RP had identified the key standards that are relevant to the UK HPR1000 C&I design. However, the lack of a comprehensive standards compliance demonstration for the centralised C&I systems is a shortfall against UK regulatory expectations, in particular against SAP ECS.3. It is encouraging that the RP has committed to further analysis during future phases, but from the documentation submitted in GDA I cannot conclude that the design of C&I systems has adequately considered the relevant standards for nuclear installations applicable to the UK.

67. I also note that the RP has not provided any demonstration of compliance of the design of the non-centralised C&I systems against the requirements of RGP. While I appreciate that these systems were out of scope for GDA, my expectation is that the post-GDA analyses will include the non-centralised C&I systems important to safety.

68. I consider that the significance of this matter is such that ONR should track it to completion, but also that the output of the analyses will depend on licensee design choices. I have therefore raised an Assessment Finding for the licensee to undertake detailed comparison analysis of the detailed design of C&I systems against relevant standards.

> AF-UKHPR1000-0024 – The licensee shall complete a compliance demonstration of the detailed design of all UK HPR1000 C&I systems important to safety, against the requirements of IEC 61513 and its normative standards. The demonstration should consider all aspects of the design lifecycle, including the processes that govern how the design is developed, and the results should inform the safety case. For any areas of non-compliance the licensee shall implement reasonably practicable measures to address the shortfalls.

69. My sample reviews of the BSCs and supporting evidential documents identified that in some cases there was a mismatch between the evidence offered and the argument that it is intended to satisfy. For example, during my sample of the RPS [PS] (Ref. 99), I noted that claims on operational life appeared to be supported by evidence of qualification testing, without reference to how operational lifetime may be simulated, estimated or calculated. This is an important point because it is essential that the evidence is suitable to support the claims and arguments in order to demonstrate that the claims have been met. I consider this to be a shortfall against the expectations of SAP SC.4, specifically point (c) of paragraph 100 of the SAPs (Ref. 2), which states the expectation that as safety case should “support claims and arguments with appropriate evidence, and with experiment and/or analysis that validates performance assumptions”.

70. While I accept that the safety case will be developed further as the design develops, I consider the importance of this shortfall to be such that it should be addressed by the licensee. This has been included as part of AF-UKHPR1000-0052 (see Section 4.11).

4.2.2 Strengths

71. The RP has developed a C&I safety case which is logically structured around a set of high-level claims. These are decomposed in a series of BSC documents into sub-claims, each of which addresses one specific aspect of the case. The BSCs provide arguments that demonstrate how the claims are addressed, and references to the underpinning evidence. It is possible to trace the ‘golden thread’ through the C&I safety case, and the rationale for the case is sufficiently clear.

4.2.3 Outcomes

72. My assessment of the structure and clarity of the C&I safety case found that the C&I aspects of the safety case are sufficiently evidential, intelligible, robust and balanced, and that the expectations of SAP SC.1 (Ref. 2) and NS-TAST-GD-051 (Ref. 12) have been adequately addressed given the current stage of design development. I judged that the RP provided a suitable and sufficient demonstration of compliance with RGP, within the context of GDA, which allowed me to close RO-UKHPR1000-0016 (Ref. 124).

73. My assessment identified three matters for resolution by the licensee; these are summarised below:

- A number of inconsistencies, limitations and dependencies in the C&I safety case were identified. While these are not considered to present an impediment to the closure of GDA, they should be reviewed and, as appropriate, addressed in detailed design and site-specific safety case development work post-GDA.
- The RP has not provided an adequate demonstration that the design of C&I systems has considered the requirements of relevant C&I standards applicable to nuclear facilities.
- The RP has not consistently demonstrated that evidence supporting claims and arguments is suitable to demonstrate that the claims are met.

74. These have been taken forward as Assessment Findings.

75. I also identified a minor shortfall against the expectations of SAP ECS.5 with regard to the referencing of evidence from the reference plant.

4.2.4 Conclusion

76. Based on the outcome of my assessment of the structure and clarity of the C&I safety case, I have concluded that the safety case is sufficiently well developed for the purposes of GDA.

77. I identified shortfalls against the expectations of SAPs SC.4 and ECS.3; I do not judge these shortfalls to be significant enough to prevent the issue of a DAC and I have therefore raised Assessment Findings for them to be addressed by the licensee.

4.3 Adequacy of C&I Architecture

4.3.1 Assessment

78. The overall C&I architecture of the UK HPR1000 is presented in Chapter 8 of the PCSR (Ref. 3) and described in greater detail in the overall C&I design specification (Ref. 54) and the C&I architecture diagram (Ref. 127). The CAE justifying the C&I architecture is provided in the 'BSC of Overall C&I Architecture' (Ref. 44). The C&I architecture comprises the following systems:

- primary protection systems, the RPS [PS] and SAS;
- a diverse secondary protection system, the KDS [DAS];
- a system dedicated to the management of severe accidents, the KDA [SA I&C];
- systems dedicated to the control and monitoring of the plant during normal operation, the PSAS and KIC [PCICS];
- several non-centralised C&I systems dedicated to the operating functions of the UK HPR1000, for example the RGL [RPICS] and RPN [NIS]; and
- HMI workstations for operator monitoring and control (see Section 4.9 for description and assessment of HMI).

79. During GDA Step 3 I undertook a high-level assessment of the adequacy of the C&I architecture (Ref. 128). In GDA Step 4 I have undertaken a more detailed review of the evidence presented by the RP to support the claims and arguments relevant to the C&I architecture. The objective of my assessment was to seek confidence that the C&I architecture design had adequately considered key safety principles, specifically the following:

- defence-in-depth;
- categorisation of safety functions and classification of systems;
- independence, diversity, redundancy, separation and segregation;
- interconnection between C&I systems;
- reliability and failure mode considerations;
- prioritisation of actuation; and

- protection against spurious actuation.

80. Table 2 below lists each of the centralised C&I systems and provides information relevant to the Category of safety function(s) that the system delivers, its safety Class, its reliability target and the plant status for which the system is claimed.

Table 2: UK HPR1000 Centralised C&I Systems

Plant Status	System	Safety Function Category (Equivalent to IEC 61226 Category)	Safety Class (Equivalent to IEC 61513 Class)	Reliability Target (Probability of failure on demand (pfd))
Normal operation	Plant Standard Automation System (PSAS)	FC3 (Category C)	F-SC3 (Class 3)	10^{-1} (NOTE 1)
	Plant Computer Information Control System (KIC [PCICS])	FC3 (Category C)	F-SC3 (Class 3)	10^{-1} (NOTE 1)
Fault conditions	Reactor Protection System (RPS [PS])	FC1 (Category A)	F-SC1 (Class 1)	10^{-4}
	Safety Automation System (SAS)	FC2 (Category B)	F-SC2 (Class 2)	10^{-3}
	Diverse Actuation System (KDS [DAS])	FC2 (Category B)	F-SC2 (Class 2)	10^{-3}
Severe accidents	Severe Accident System (KDA [SA I&C])	FC3 (Category C)	F-SC3 (Class 3)	10^{-1}

NOTE 1 – The PSAS and KIC [PCICS] are both continuous mode systems and the reliability targets claimed are therefore quoted in terms of the probability of failure per year rather than pfd

4.3.1.1 Categorisation of Safety Functions and Classification of SSCs

81. I wanted to establish confidence that the UK HPR1000 C&I systems are appropriately classified for the safety functions that they deliver. The relevant SAPs (Ref. 2) for this aspect of my assessment were ECS.1 and ECS.2.

82. The RP's methodology for the categorisation of safety functions and classification of SSCs is documented in 'Methodology of Safety Categorisation and Classification' (Ref. 129), and the approach to allocation of functions to C&I systems, as described in 'Functional Assignment of I&C Systems' (Ref. 130), is that safety functions are derived from the fault schedule (Ref. 131). This identifies the level of protection required against each initiating event. Deterministically for frequent faults, two independent lines of protection are required, placing a requirement for diversity and separation on the C&I systems delivering the primary and secondary safety functions.

83. In consultation with the ONR Fault Studies specialist I reviewed the above listed documents and judged that the safety function categories specified in the fault schedule (Ref. 131) are appropriate, that the safety classifications assigned to the centralised C&I systems are commensurate with the safety function categories and that the expectations of NS-TAST-GD-094 (Ref. 13) had been met. The full assessment of the safety analysis is provided in the Fault Studies area (Ref. 132).

84. I sampled the non-centralised C&I systems, seeking confidence that their safety classification was commensurate with the significance of the safety functions that they perform.

85. The system design manual for the RPN [NIS] (Ref. 133) states that the system is Class 1, on the basis that it plays a principal role in the delivery of the Category A reactor trip function, as well as other safety functions of a lower category. I judge this to be an appropriate classification.

86. The system design manual for the KRT [PRMS] (Ref. 134) states that the system is Class 1 on the basis that the monitoring functions relating to steam generator leakage, reactor pool and spent fuel pool are Category A. I judge this to be an appropriate classification.

87. My review of revision C of the system design manual for the RIC [IIS] (Ref. 135) found that the system had been assigned a classification of Class 2, on the basis that it performs the measurement of core outlet temperature, which is a Category B function. Whilst I was content with the overall system classification, the ONR fuel and core assessment (Ref. 136) raised concerns that the self-powered neutron detector (SPND) sub-system had not been assigned a safety classification despite the fact that the sub-system supports the calibration of the ex-core neutron flux detectors, which are part of the RPN [NIS] and perform Category A functions. I worked with the ONR fuel and core inspector to engage with the RP on this matter; this engagement resulted in the RP raising modification M58 (Ref. 137) to raise the classification of the SPND sub-system to Class 3. I judge to be an appropriate classification based on the guidance in NS-TAST-GD-094 (Ref. 13), as the sub-system plays a supporting role in delivery of a Category A safety function. The latest version of the system design manual (Ref. 138) reflects this revised classification.

88. The system design manual for the RGL [RPICS] (Ref. 139) states that the system is decomposed into two sub-systems: the rod position indication system that is classified as Class 1 on the basis that it monitors and indicates the position of control rods in the core, which is a Category A function; and the rod control system, which is classified as Class 3 on the basis that it received commands from the PSAS to control the insertion or withdrawal of rod clusters, which is a Category C function. I judge these classifications to be appropriate. The design of the RGL [RPICS] is outside of GDA scope and I have therefore not assessed the means by which independence between the two sub-systems is achieved.

89. Based on the outcomes of my assessment I am content from a C&I perspective that the RP has appropriately categorised safety functions and has assigned appropriate classifications to the UK HPR1000 C&I systems, and that the expectations of SAPs ECS.1 and ECS.2 have been met.

4.3.1.2 C&I System Reliability and Failure Modes

90. I sought to establish confidence that the UK HPR1000 C&I systems can achieve the required reliability, and the methodologies used by the RP to demonstrate reliability. The key SAPs (Ref. 2) that informed this aspect of my assessment included ERL.1, ERL.2 and ESS.21 – in particular paragraph 416.

91. My GDA Step 3 C&I assessment (Ref. 128) identified a shortfall in the C&I safety case in that the link between the fault schedule and the C&I reliability targets was not clear. Subsequently, in Step 4 the RP submitted a document titled ‘Reliability Targets of the I&C Systems for UK HPR1000’ (Ref. 140) . I reviewed this document and found that it was still not clear how the detailed fault analysis had been considered in the assignment and validation of reliability targets. I therefore raised RQ-UKHPR1000-1377 (Ref. 109) seeking further explanation from the RP.

92. The RP's response to this RQ explained how the C&I reliability targets have been informed by the frequency of initiating faults that are quoted in the fault schedule, and how the analysis represents a bounding case scenario for the combination of safety systems required to ensure safety function delivery. The response also stated that the fault analysis does not place any claim on the reliability of the PSAS in supporting the core damage frequency; the reliability of 10^{-1} pfd is claimed on the basis that the PSAS performs FC3 (Category C) safety functions. I was content with this response.

93. In GDA Step 4 the RP undertook an analysis to demonstrate that the UK HPR1000 C&I systems will meet their reliability targets (Ref. 141). Through GDA Step 3 and Step 4 the RP also submitted examples of hardware reliability studies, in the form of failure modes and effect analysis (FMEA), for the RPS [PS] (Ref. 114), KDS [DAS] hardware platform (Ref. 97) and a sample of components of the FirmSys platform (Ref. 96). Assessment of these documents by the ONR TSC identified several issues which I judge to be significant (Ref. 38). These can be summarised under the following themes:

- the methodologies by which FMEA are undertaken and how these have considered RGP;
- the clarity of relationship between platform-level and system-level FMEA;
- the level of detail to which FMEA are applied;
- the validity and relevance of component failure data used; and
- how the outputs of FMEA are fed back into the system and architecture design.

94. To address these concerns I raised several RQs (i.e. RQ-UKHPR1000-0363, 1061, 1144, 1145, 1167 and 1528 (Ref. 109)) over the course of GDA Step 3 and Step 4. The responses to these RQs, in addition to a revised C&I reliability study (Ref. 57) provided sufficient clarification and justification that, based on the preliminary designs presented in GDA, the C&I systems will be capable of meeting their reliability targets. The RP also provided descriptions of further reliability analyses that will be undertaken post-GDA, as the system designs develop. While I was content that the information provided was sufficient for GDA, I considered the lack of a properly underpinned reliability study to be a shortfall which should be resolved. In particular, the analyses submitted during GDA do not provide sufficient clarity on the following aspects:

- The boundaries of the analyses as well as any assumptions and constraints.
- Identification of hazards, such as those caused by internal failures or faults, their consequences on system operation, and the measures to control these.
- The extent to which factors that may affect reliability, including self-supervision capabilities, requirements for proof testing and maintenance, etc. have been considered.
- Demonstration that faults originating in lower-class systems cannot adversely affect the operation of higher-class systems.
- Justification of the validity of underpinning data.

95. The ability to conduct detailed reliability analysis will depend on detailed design information beyond what can reasonably be expected during GDA. I have therefore raised an Assessment Finding for this to be addressed by the licensee.

AF-UKHPR1000-0026 – The licensee shall demonstrate that the hardware reliability of the detailed design of the UK HPR1000 C&I systems fulfils the requirements derived from the safety analysis. The hardware reliability analyses should follow a methodology that is informed by international standards and relevant good practice. The analyses should give particular consideration to the following as a minimum:

- clear definition and justification of the boundaries of the analyses, including any assumptions and constraints;

- the identification of hazards, such as those caused by internal failures or faults, their consequences on system operation, and the measures to control these; and
- the identification of all factors that may affect reliability, including self-supervision capabilities, requirements for proof testing and maintenance.

4.3.1.3 Independence Between C&I Systems

96. A key aspect of my assessment was the consideration of whether the C&I architecture incorporates sufficient independence between systems, such that the failure of one system or component does not lead to the loss of multiple layers of defence. The relevant SAPs (Ref. 2) to this area of assessment include:

- EKP.3 Defence-in-depth;
- EDR.2 Redundancy, diversity and segregation;
- EDR.3 Common cause failure;
- EDR.4 Single failure criterion;
- ELO.4 Minimisation of the effects of incidents;
- ESS.1 Provision of safety systems;
- ESS.7 Diversity in detection of fault sequences;
- ESS.18 Failure independence;
- ESS.20 Avoidance of connection to other systems; and
- EES.5 Cross-connection to other services.

97. My assessment of the independence between C&I systems was informed by relevant RP submissions, including:

- 'Independence Analysis of I&C Systems' (Revision D) (Ref. 142).
- 'Optioneering Analysis Report for CIM Improvement' (Revision B) (Ref. 143).
- 'Optioneering Analysis Report for SPM Improvement' (Revision B) (Ref. 144).
- 'BSC of Overall I&C Architecture' (Revision F) (Ref. 44).
- 'BSC of Protection System' (Revision F) (Ref. 99).

98. My Step 3 assessment (Ref. 128) identified a number of significant shortfalls in the level of independence between C&I systems which presented a risk that CCF could simultaneously affect multiple systems across different levels of DiD. I therefore raised RO-UKHPR1000-0017 'Demonstration of independence between C&I systems' (Ref. 40) which identified five actions for the RP to address the shortfalls, as follows:

- to provide a suitable and sufficient justification for the sharing of equipment between C&I systems important to safety;
- to provide a suitable and sufficient justification for the role of the component interface module (CIM) in delivery of safety functions for multiple C&I systems;
- to provide a suitable and sufficient justification for the role of the signal pre-processing module (SPM) in delivery of safety functions for multiple C&I systems;
- to provide a suitable and sufficient justification for the approach to separation and segregation of C&I systems to protect against consequential physical effects caused by faults and normal actions within other systems and internal plant hazards; and
- to provide a suitable and sufficient justification of how the UK HPR1000 C&I architecture provides sufficient independence such that the risk of failures affecting multiple systems and compromising delivery of safety functions is reduced ALARP.

99. During GDA Step 4 the ONR Fault Studies specialist inspector raised RO-UKHPR1000-0023 'Demonstration of Diverse Protection for Frequent Faults' (Ref. 40), which identified a number of shortfalls in the provision of diverse protection for frequent

faults. RO-UKHPR1000-0017 is closely related to RO-UKHPR1000-0023, and I therefore worked closely with ONR specialists from Fault Studies in support of my assessment. My assessment of RO-UKHPR1000-0017 is documented in an assessment note (Ref. 145); the key outcomes are detailed in the following sub-sections.

Sharing of Field Equipment

100. During GDA Step 4 the RP provided an analysis of the independence within the C&I architecture (Ref. 142), which documented the analysis of equipment shared between C&I systems. This included sensors, actuators, electrical supplies and heating, ventilation and air conditioning (HVAC) systems, as well as interconnections and communications between systems. The document listed all of the protection functions in the UK HPR1000 fault schedule and against each function identified the signals that initiate these functions on the RPS [PS] and diverse actuation system KDS [DAS]; this identified several instances where there is no signal diversity between the two systems.

101. The RP undertook an optioneering analysis to evaluate options for modification of the C&I architecture to introduce additional diversity in the sensors shared between C&I systems at different DiD levels. The analysis identified instances where sensors are shared between the RPS [PS] and KDS [DAS], and identified a series of modifications whereby additional signal diversity would be implemented in one of the following three ways:

- the highest priority modification being the implementation of sensors measuring different physical parameters within the RPS [PS] and KDS [DAS] (i.e. prioritising parameter diversity);
- where this was judged not reasonably practicable, the implementation of redundant and diverse sensors for the KDS [DAS] to provide diverse measurement; and
- where this was judged not reasonably practicable, diversity will be achieved through the diversification of sensors between different divisions of the RPS [PS] and KDS [DAS].

102. The C&I independence analysis (Ref. 142) also identifies instances where actuation devices are shared between the RPS [PS] and KDS [DAS], and provides references to documentation detailing the optioneering to select preferred options for the provision of diverse actuation.

103. The RP implemented design modification M37 (Ref. 146) to implement the preferred options for diverse sensors and actuators. In consultation with ONR specialist inspectors from Fault Studies and Mechanical Engineering I conducted a sample review of the documentation associated with these modifications (Ref. 147), (Ref. 148), (Ref. 149), (Ref. 150) and (Ref. 126). Based on the evidence sampled I was content that the optioneering undertaken was suitably rigorous and that the modifications have addressed shortfalls in the independence and diversity of sensors and actuators. These modifications have been implemented within GDA.

104. From my sample assessment, and in consultation with the Fault Studies specialist, I identified one case where in certain operating states there may not be diverse detection of a fault. Specifically, against the fault ”Steam Generator Tube Rupture (One Tube) (State A)”, the fault schedule (Ref. 131) lists the protection parameters for the reactor trip function as pressuriser pressure and steam generator level (narrow range).

105. While these are diverse physical parameters, the ‘RPS [PS] System Requirements Specification’ (Ref. 151) states that these parameters are both interlocked with

permissive signals which means they are inhibited in certain operational states. The RP has not provided a justification that the setpoints of these parameters cover the full range of operations, or demonstrated that the permissive interlocks cannot compromise fault detection. I judge this to be a shortfall against SAP ESS.7. My expectation is that the licensee will give further consideration to the configuration of permissive signals during the detailed C&I design, and therefore do not consider that this shortfall needs to be addressed in GDA. However, I do consider its significance to be such that it should be tracked to resolution. Further discussion of permissive signals is provided in Section 500, and this issue has been captured as part of Assessment Finding AF-UKHPR1000-0049 (see Section 500).

106. The 'Independence Analysis of I&C Systems' (Ref. 142) also identifies that sensors are shared between the RPS [PS] and the plant standard automation system (PSAS), and details the optioneering undertaken "to determine the configuration of sensors shared between the RPS [PS] and PSAS which reduces risks ALARP". The study concludes that it is not reasonably practicable to implement diverse sensors between the RPS [PS] and the PSAS, and that the current design scheme provides adequate risk reduction. The following reasons were provided as justification:

- The sensors utilised by the RPS [PS] and the PSAS deploy three-fold or four-fold redundancy to reduce the risk of failure of a single sensor leading to concurrent loss of safety function delivery between the RPS [PS] and PSAS.
- All sensors shared between the RPS [PS] and PSAS are classified as Class 1.
- The RPS [PS] and PSAS are functionally independent from each other and the role of the SPM prevents adverse interactions between the two systems.
- Other reactor designs to have completed GDA have implemented similar design schemes whereby sensors are shared between the primary protection system and plant control system.

107. The 'Independence Analysis of I&C Systems' (Ref. 142) states that "the RPS [PS] and PSAS do not share actuators".

108. Having reviewed the evidence I was content that the optioneering was sufficiently rigorous and the conclusions were adequately underpinned. On the basis of the evidence sampled I was satisfied that the RP had demonstrated that failure of sensors on the PSAS will not result in the failure of RPS [PS] safety functions.

Diversity of Support Systems

109. As part of RO-UKHPR1000-0023 (Ref. 40) the RP identified a need to improve the levels of diversity within the HVAC systems. The identified shortfalls and optioneering carried out are documented in (Ref. 152) and (Ref. 153). The RP has addressed these shortfalls by implementing modification M35 (Ref. 154). From a C&I perspective I was content that the modification will ensure that there is adequate DiD and diversity within HVAC systems that support the centralised C&I systems. The detailed assessment of the HVAC systems is provided in the Mechanical Engineering assessment report (Ref. 155).

110. The 'Independence Analysis of I&C Systems' (Ref. 142) lists the electrical systems that provide power to each of the centralised C&I systems. I participated in a technical meeting with the ONR Electrical Engineering specialist inspector (Ref. 156) where the RP presented the approach to allocation of the centralised C&I systems to electrical power systems. Following this meeting the Electrical Engineering inspector raised two RQs seeking clarification on the proposed design scheme.

111. Of particular relevance to my assessment was RQ-UKHPR1000-0676 (Ref. 109) which raised concerns on the RP's proposal for the F-SC3 (Class 3) severe accident C&I system to be supplied from a non-classified electrical system. In response to this RQ

the RP undertook an optioneering exercise which identified alternative power supplies to the severe accident system from appropriately classified equipment. I consulted with the ONR Electrical Engineering inspector who confirmed that he was content with the revised design scheme (Ref. 157).

112. On the basis of the evidence sampled and my consultation with the ONR Electrical Engineering inspector I was content that there is adequate independence between the electrical power supplies to the centralised C&I systems such that failure of a single electrical system will not affect multiple layers of defence.

113. Based on the outcomes of my assessment I judge that the RP has provided a suitable and sufficient justification of the sharing of equipment between C&I systems important to safety.

CIM Design Scheme

114. The role of the CIM is to perform priority management of control and actuation commands arising from the centralised C&I systems. The expectation of RO-UKHPR1000-0017 (Ref. 40) was for the RP to produce a suitable and sufficient justification of the role of the CIM in delivery of safety functions for multiple C&I systems which considers the architecture and implementation technology of the CIM, and demonstrates that the risk of failure of the CIM affecting multiple divisions within a C&I system, and multiple levels of DiD, is reduced ALARP.

115. During GDA Step 4 the RP undertook an optioneering exercise to select a revised design scheme for implementation of the CIM; this was documented in 'Optioneering Analysis Report for CIM Improvement' (Ref. 143). The document described three potential CIM design schemes; one based on complex programmable logic devices (CPLD) (this is the CIM design from the reference plant), one based on microprocessor technology and one based on simple hardware technology. It set out several configuration options, of the three design schemes, varying between primary and secondary system and/or inter-divisional system diversity to provide adequate diversity within the architecture.

116. The 'long list' of options was assessed against a set of preliminary screening criteria, to filter out those options that would not be reasonably practicable to implement. The remaining 'short-list' options were then evaluated against a detailed set of criteria to identify a preferred option to be taken forward. The study concluded that the preferred option is for a combination of CPLD and simple hardware-based CIM modules to be implemented through the architecture. The document went on to set out for each safety function how the CIM modules will be configured across each division.

117. Having assessed the document I was content that the RP had undertaken a rigorous optioneering exercise, that the evaluation criteria were suitable and had been applied in a consistent manner, and that the option to be taken forward is appropriate. However, it was not clear how the CIM configuration had been optimised for each safety function. I therefore raised RQ-UKHPR1000-0887 (Ref. 109) requesting clarification in this regard.

118. The response to this RQ described that the process of CIM allocation is informed by the 'Function Analysis Report for Diverse Protection Line Design' (Ref. 147) and used an example safety function to explain the process. While the explanation was helpful it was still not clear how the allocations had been demonstrated to meet the requirements of the fault analysis for all safety functions. I therefore raised RQ-UKHPR1000-1115 (Ref. 109) to seek further clarification.

119. In response the RP provided a comprehensive explanation of how it had confirmed that the CIM configurations met the requirements of the fault analysis, using further examples to support the demonstration. I was content with this response.

120. The modification to the CIM design scheme was submitted to ONR under modification M30 (Ref. 158). I reviewed the modification documentation for M30 and I was content that it reflected the outcomes of the optioneering study, and that the modification provides adequate independence and diversity within the CIM architecture. While I am satisfied that the concept design information provided is sufficient for GDA, I consider it important to ensure that the detailed design of the modified CIM is implemented in accordance with this concept. I have therefore raised an Assessment Finding for ONR to track this to completion.

AF-UKHPR1000-0027 – The licensee shall demonstrate that the detailed designs for both the diverse Component Interface Module and Signal Pre-processing Module provide resilience to common cause failures and shall develop detailed designs for those modules in accordance with the concept design provided in GDA, or equivalent alternatives.

121. Based on the outcomes of my assessment I am content that the RP has provided a suitable and sufficient justification for the role of the CIM in delivery of safety functions for multiple C&I systems.

SPM Design Scheme

122. The SPM is responsible for acquisition and pre-processing of signals from sensors and their distribution to the centralised C&I systems. The expectation of RO-UKHPR1000-0017 (Ref. 40) was for the RP to produce a suitable and sufficient justification of the role of the SPM in delivery of safety functions for multiple C&I systems which considers the architecture and implementation technology of the SPM and demonstrates that the risk of failure of the SPM affecting multiple divisions within a C&I system, and multiple levels of DiD, is reduced ALARP.

123. During GDA Step 4 the RP undertook an optioneering exercise to select a revised design scheme for implementation of the SPM; this was documented in 'Optioneering Analysis Report for SPM Improvement' (Ref. 144). I assessed this report and found that the RP had followed the same process as that for the CIM optioneering analysis (see paragraphs 116 and 117). The report concludes that the preferred option is to provide two diverse SPM modules, both of which are based on simple hardware technology: SPM-1 incorporates magnetic isolation (this is the SPM design for the reference plant), and SPM-2 uses capacitive isolation.

124. The optioneering analysis also sets out the configuration of SPM modules across divisions for each safety function. My review found that this did not appear to consider the reliability targets identified in the fault analysis, whereas the CIM optioneering analysis had done so. I therefore raised RQ-UKHPR1000-1398 (Ref. 109) to ask how reliability targets have been considered in the optimisation of SPM configuration.

125. The RP's response explained that the configuration of SPMs has taken account of the diversification of protection parameters (described in paragraphs 100 – 103) and provided a revised table showing the reliability targets for the combination of SPM for each safety function. I was satisfied that this response demonstrated that the RP had followed the same process for SPM configuration as was followed for the CIM.

126. I was content that the RP had undertaken a comprehensive optioneering exercise to address the identified shortfall, and that the design modification to introduce diverse SPM will result in a significant safety improvement that will provide adequate independence and diversity within the SPM architecture.

127. The modification to the SPM design scheme was submitted to ONR under modification M90 (Ref. 159). I reviewed the modification documentation for M90 and was content that it reflects the outcomes of the optioneering study, and that the modification provides adequate independence and diversity within the SPM architecture. While I am satisfied that the concept design information provided is sufficient for GDA, I consider it important to ensure that the detailed design of the modified SPM is implemented in accordance with this concept. This is included as part of AF-UKHPR1000-0027 (see sub-section 4.3.1.3).

128. Based on the outcomes of my assessment I am content that the RP has provided a suitable and sufficient justification for the role of the SPM in delivery of safety functions for multiple C&I systems.

Interconnections Between C&I Systems

129. I sampled the potential for failure of lower-class systems to affect higher-class systems. I found that the 'Independence Analysis of I&C Systems' (Ref. 142) had identified the interconnections between the centralised C&I systems, grouped them into five categories and sets out how separation is achieved for each category. The analysis also identified interconnections between redundant channels or divisions of the same system, and again set out the isolation methods employed to achieve independence.

130. The RP's general principles for isolation are summarised below:

- Hardwired links are protected via electrical isolation; for analogue signals this is performed by the SPM, while discrete signals are isolated through the use of relays.
- Communication links are protected through a combination of optical isolation and the use of separate communications modules to provide a buffering function.

131. In determining the isolation methods the RP has undertaken an ALARP assessment which has considered a number of factors including the requirements for each connection, the safety function(s) that each connection supports, and the requirements and expectations of RGP to provide a justification that the design provides adequate protection against failure propagation.

132. The C&I design specification (Ref. 54) identifies the interfaces between the non-centralised and centralised C&I systems. I reviewed this document and found that the same principles of isolation have been applied to these interfaces.

133. On the basis of the evidence reviewed I was content that the RP had identified the interconnections within the C&I architecture – both between centralised systems and to and from non-centralised systems – and has put in place measures to protect against propagation of failures between systems and between redundant channels and divisions of the same system. While the information provided is sufficient for GDA, my expectation is that during the detailed design phase the licensee will undertake a comprehensive failure modes analysis to identify whether any further measures to prevent propagation of failures can reasonably be implemented, and to demonstrate that faults originating in lower-class systems cannot compromise the operation of higher-class systems. This should be addressed as part of Assessment Finding AF-UKHPR1000-0026 above.

Separation and Segregation of C&I Systems

134. I reviewed the 'Independence Analysis of I&C Systems' (Ref. 142) seeking justification of the approach to separation and segregation of C&I systems to protect against

consequential physical effects caused by faults and normal actions within other systems and internal plant hazards.

135. To address physical segregation of C&I systems, the C&I Independence Analysis (Ref. 142) provides an assessment of the resilience of the C&I architecture against CCF due to internal hazards. The following internal hazards are considered:

- internal fire;
- internal explosion;
- internal flooding;
- high energy pipe failure;
- internal missiles;
- dropped loads;
- electromagnetic interference (EMI); and
- toxic gases and corrosive materials.

136. To inform the assessment the RP refers out to the detailed hazard assessments produced in the Internal Hazards topic area. I undertook a sample review of these documents (Ref. 160), (Ref. 161) and (Ref. 162) and was content that the information was consistent with that presented in the independence analysis.

137. I noted that the independence analysis (Ref. 142) did not discuss how the separation and segregation of C&I equipment had been influenced by the assessment of external hazards. As the detailed plant layout design progresses it is my expectation that the location of C&I equipment will be informed by external hazards. This is addressed by AF-UKHPR1000-0029 (see below).

138. The independence analysis (Ref. 142) sets out the principles that the RP has applied to the separation and segregation of C&I equipment and systems (i.e. sensors and instrumentation, equipment cabinets, human-machine interfaces, and cabling). I reviewed these and judged them to be appropriate. The document also details the assessment of susceptibility to each of the hazards listed in paragraph 135, which identified 5 specific vulnerabilities within the current design. These are listed below:

- Some sensors connected to redundant channels of the RPS [PS] are co-located within ‘exception to segregation’ areas (i.e. where the principles of separation and segregation cannot be practicably applied).
- Equipment cabinets for systems at different DiD levels within the same division are co-located.
- Cables for systems at different DiD levels within the same division are routed together.
- There are no specific separation requirements for location of equipment sensitive to EMI in relation to equipment with the highest potential for generation of EMI.
- No operational restrictions are specified for the use of portable EMI sources.

139. An optioneering exercise was undertaken to determine suitable options to address these vulnerabilities. The outcomes of this are summarised in the below paragraphs.

140. The RP considered options for relocation of sensors associated with the steam generator level (narrow range) signals and concluded that it would not be reasonably practicable to modify the reference design. The justification for this is given as:

- Adjacent rooms are in a higher category radiation protection area which would result in a significant increase in radiation exposures to maintenance workers.
- Relocation would result in additional design complexity as modifications to fire protection and HVAC systems would be required.

- The use of redundant, functionally diverse signals for RPS [PS] functions means that there would be an additional means of fault detection in the event of CCF of the steam generator level (narrow range) sensors.

141. I reviewed the detailed optioneering sheet associated with this gap (included as an appendix in 'Independence Analysis of I&C Systems' (Ref. 142)) and was content that the conclusions were adequately underpinned. However, I noted that the RP had only considered the potential relocation of the steam generator level (narrow range) sensors and had not considered other sensors that are identified as being located in 'exception to segregation' areas. A forward action was identified for this to be addressed during detailed design through further detailed optioneering. Given that the plant layout will not be finalised until site-specific stages I am content that the work done in GDA is sufficient. However, I consider it important to ensure that the licensee undertakes this optioneering. This is addressed as part of Assessment Finding AF-UKHPR1000-0029 (see below).

142. The RP also considered options for increasing the spacing between C&I cabinets within room BSC3729ZRE of division C, in order to improve separation between C&I systems at different DiD levels. The optioneering concludes that modifying the layout from the reference design would not be reasonably practicable, with the justification being given as:

- The additional cabling required would increase the fire loading, consequently increasing the risk that a fire could propagate to affect multiple systems.
- Relocation of C&I cabinets would result in additional design complexity with re-design of structures and cable routes required.
- There would be a negative impact on human factors relating to maintenance as access would be more restricted.
- The current GDA plant layout places the C&I cabinets, associated with the KDS [DAS] and RPS [PS] in separate rooms, resulting in a low likelihood that a hazard would coincidentally impact both systems.

143. I reviewed the detailed optioneering sheet associated with this shortfall (included as an appendix in 'Independence Analysis of I&C Systems' (Ref. 142)) and was satisfied with the arguments presented. However, I noted that the RP had only considered division C and not cabinets within other divisions. A forward action was identified for this to be addressed during detailed design through further detailed optioneering. My expectation is that this optioneering will give further consideration to whether the separation and segregation of C&I cabinets can be improved in all divisions. Given that the plant layout will not be finalised until site-specific stages I am content that the work done in GDA is sufficient. However, I consider it important to ensure that the licensee undertakes this optioneering. This is addressed as part of Assessment Finding AF-UKHPR1000-0029 (see below).

144. The consideration of options for separation of cable routes for different systems within the same division concluded that there were no reasonably practicable solutions that would reduce risk. The RP's justification can be summarised as follows:

- Cables are separated by division.
- Some degree of cable separation within divisions is achieved in the reference design, with cables separated into different trays according to their voltage levels.
- Where cables belonging to different systems are routed together they are all rated and qualified to the same level as cables associated with Class 1 systems.
- Further separation will result in increased design complexity and, in some locations, there is no available space for the installation of additional cabling, thus presenting a risk to constructability.

145. Having reviewed the optioneering presented in the independence analysis I was content that, given the early stage of design, the RP has given sufficient consideration to the separation of cabling for GDA. However, insufficient evidence was presented to underpin the arguments presented and I am therefore of the opinion that, as the design develops in subsequent phases, further analysis should be undertaken, further analysis should be undertaken to consider opportunities to improve the cable routing design. I have therefore identified this as part of Assessment Finding AF-UKHPR1000-0029 (see below).

146. Regarding the shortfalls associated with EMI, the independence analysis specifies a series of control measures to be implemented during site specific phases, including the formal specification of requirements for the separation of sensitive equipment from sources of EMI and operational constraints, in order to manage the hazard. Forward actions are identified to undertake detailed assessment and optimisation of measures during detailed design. Having reviewed the information provided I was satisfied that the RP had identified a set of reasonable and practicable requirements to reduce the risk of EMI induced faults. I support the RP's conclusion that detailed assessment and definition of control measures should take place during site-specific stages, although I am of the opinion that it is important to ensure that the measures are adequately implemented. I have therefore raised an Assessment Finding for the licensee to ensure that this is addressed.

AF-UKHPR1000-0029 – The licensee shall, as part of detailed design of all UK HPR1000 C&I systems important to safety, determine whether additional measures to provide separation and segregation to protect against consequential effects caused by internal and external plant hazards are reasonably practicable. The analysis should include, but not be limited to, the following:

- separation and segregation of sensors located in 'exception to segregation' areas.
- separation and segregation of C&I cabinets associated with different systems.
- separation and segregation of cable routes for different systems within the same division; and
- control measures to reduce the risk of electromagnetic interference and radio frequency interference induced faults.

147. Based on the outcomes of my assessment I judge that justification for the approach to separation and segregation of C&I systems is sufficient for GDA.

Justification of Architecture Design

148. As part of the response to RO-UKHPR1000-0017 the RP provided the Revision F of 'BSC of Overall I&C Architecture' (Ref. 44) which sets out the CAE to demonstrate the adequacy of the C&I architecture, including independence between systems. The RP also provided Revision C of 'BSC of Protection System' (Ref. 118) as an example of the demonstration of independence at the system level.

149. I reviewed the architecture BSC and found that it includes CAE relevant to the demonstration of how independence, diversity and DiD is achieved in the design of the C&I architecture. These include arguments related to the sharing of components, diversification of support systems, interconnections between systems, and separation and segregation. I was content that the information presented is consistent with the evidence presented in the C&I independence analysis (Ref. 142) and other documentation discussed in my assessment of RO-UKHPR1000-0017 (Ref. 145).

150. My review of the BSC for the RPS [PS] (Ref. 118) found that the CAE in relation to independence and diversity are similar to those presented at the architecture level,

with more specific argumentation provided as to how the design of the RPS [PS] supports the independence and diversity in the C&I architecture.

151. While I was generally content that the claims and arguments were consistent through the safety case, I noted that some interconnections between the RPS [PS] and other systems were not identified in the BSC. I therefore raised RQ-UKHPR1000-1594 (Ref. 109) seeking further information on the nature of these interfaces and how independence is assured. The RP's response provided explanations of the functionality of the interfaces and the means by which signal isolation is achieved. The RP also updated the BSC to Revision E, reflecting the RQ response (Ref. 163). Revision F of the BSC was submitted later in GDA Step 4 to reflect further development of the safety case (Ref. 99).

152. On the basis of my assessment of the response to RO-UKHPR1000-0017 (Ref. 40) I was content that the RP has provided a suitable and sufficient demonstration of the independence between systems in the UK HPR1000 C&I architecture and on this basis the RO was closed (Ref. 145).

153. I am content that the design of the C&I architecture supports the plant's approach to defence-in-depth and diversity. The RP has demonstrated that there is adequate independence between C&I systems, and between redundant channels/ divisions within systems and has implemented design modifications to address shortfalls in diversity between systems. On the basis of the evidence sampled I am content that, from an architectural perspective, SAPs EKP.3, EDR.2, EDR.3, EDR.4, ESS.1, ESS.18, ESS.20 and EES,5 have been satisfactorily addressed for GDA. I identified a shortfall against the expectations of SAP ELO.4; this has been taken forward as Assessment Finding AF-UKHPR1000-0029.

4.3.1.4 Spurious C&I Actuation

154. I worked closely with the ONR Fault Studies specialist inspector to assess the RP's analysis of the consequences of spurious actuation of C&I systems. The key SAPs (Ref. 2) that were considered in this assessment included ESS.17 and ESS.22.

155. During GDA Step 3 the RP provided its methodology for the identification of postulated initiating events (PIE) (Ref. 164) and the list of PIEs related to spurious C&I actuation (Ref. 165). I reviewed these submissions and my findings are summarised below:

- The RP had provided a detailed description of the analysis methodology, including the scope of systems analysed and the principles for screening out of functional groups.
- The methodology considered relevant good practice in the form of the Multinational Design Evaluation Programme (MDEP) common position on spurious actuation (Ref. 166).
- The RP had grouped PIEs into functional groups, some of which were screened out following analysis. For those functional groups screened out a justification was provided.
- The RP identified a total of 97 PIEs that could not be screened out. These were then subject to a bounding case analysis against list of design basis conditions (DBC).

156. At the end of GDA Step 3 the PIE bounding case analysis had not been undertaken. I therefore stated the expectation in my Step 3 assessment (Ref. 128) that the RP would complete this analysis and identify any required design changes to protect against PIEs that are not bound by the fault analysis.

157. The bounding case analysis for spurious C&I actuation was presented in GDA Step 4 (Ref. 167); this presented the analysis methodology, stated the assumptions on which

the analysis was based and provided the results of the analysis. The conclusions of the analysis are summarised below:

- PIEs as a result of spurious actuation of the PSAS, KDS [DAS] or non-centralised C&I systems are bounded by existing design basis faults, and the safety functions provided by the RPS [PS] and SAS can still be delivered.

- PIEs as a result of spurious actuation of the RPS [PS] or SAS are not bounded by existing design basis faults and therefore new fault conditions are created. In particular the analysis concludes that spurious actuation of RPS [PS] or SAS with the reactor at power could lead to an anticipated-transient-without-scram (ATWS) accident. A total of 17 PIEs fall into this category.

158. The RP undertook further analysis to demonstrate that these events can be mitigated and protected against by the C&I safety systems (Ref. 168). This concluded that the KDS [DAS] is capable of providing protection and mitigation for the fault conditions initiated by spurious actuation of the RPS [PS] and SAS.

159. Having reviewed the analysis documents I sought clarification of how the operation of the CIM would support the protection against faults arising from spurious C&I actuation. I raised RQ-UKHPR1000-0815 (Ref. 109) asking the RP to provide a detailed description of the CIM priority logic, and to justify how the logic ensures that all safety functions can be delivered in the event of failure of one C&I system.

160. While the response provided useful clarification I noted that it stated that a spurious actuation of plant components caused by the RPS [PS] cannot be corrected by lower priority systems without the need for manual intervention by the operator, either through operation of hardwired switches within the MCR, or through local actuation at the CIM cabinet. I was concerned that the need for manual intervention could prevent the timely delivery of safety functions and hence raised RQ-UKHPR1000-0974 (Ref. 109) requesting further justification.

161. The RQ response provided an explanation of how the manual actuation would be performed, using an example fault to make a demonstration. The response also stated that manual actuation was within allowable grace periods from the human factors analysis, that the fault analysis of spurious actuation had taken account of these grace periods and that it demonstrated the acceptance criteria of the accident analysis had been satisfied. The RP also committed to provide further quantitative analysis during site specific phases. This has been captured as Assessment Finding AF-UKHPR1000-0157 in the Fault Studies assessment report (Ref. 132).

162. In my assessment of the response to RQ-UKHPR1000-0974 (Ref. 109) I consulted with the ONR specialist inspectors from Fault Studies and Human Factors, who were content with the justification provided by the RP. From a C&I perspective I was content that, because CIM status is reported to the MCR, operators will be alerted to the presence of a fault and the consequent need to take action. Note, the responses to RQ-UKHPR1000-0815 and RQ-UKHPR1000-0974 did not specify whether the CIM status is reported to the RSS. However, as this was not a focus of this area of my assessment I did not consider it further in GDA.

163. From a C&I perspective I am content that the RP's assessment of the consequences of spurious C&I actuation is adequate for GDA and that the expectations of SAPs ESS.17 and ESS.22 have been satisfactorily addressed. Further detailed assessment of the analysis of spurious actuation is provided in the Fault Studies assessment report (Ref. 132).

4.3.1.5 Protection Against Solar Energetic Particles

164. During GDA Step 2 ONR raised RO-UKHPR1000-0002 'Demonstration that the UK HPR1000 Design is Suitably Aligned with the Generic Site Envelope' (Ref. 40), which required the RP to provide a demonstration that the generic UK HPR1000 design is suitably aligned with the generic site envelope. ONR's assessment of the response to this RO was led by the ONR External Hazards specialist inspector. I provided support to this assessment, specifically in the RP's demonstration of the protection of C&I systems against solar energetic particles (SEP). The detailed assessment is documented in an assessment note (Ref. 169) and the External Hazards assessment report (Ref. 170), and is not repeated here. The findings of my assessment are summarised below.

165. The RP undertook an analysis of the vulnerability of C&I systems against SEP (Ref. 171). I assessed this together with the ONR External Hazards inspector and found the following:

- the methodology for the SEP vulnerability analysis was appropriate;
- the scope of the analysis was commensurate with ONR's expectations and includes the centralised C&I systems and relevant support systems;
- the depth of the analysis was adequate given the level of detail available in GDA, particularly for support systems where component selection will not take place until site-specific phases;
- the RP identified a set of control measures (to be implemented by the licensee) to protect against the hazard, including equipment diversity, physical protection to attenuate neutron flux, and the use of detection systems to alert operators of the existence of the hazard; and
- there was sufficient information presented to demonstrate that the conclusions were underpinned.

166. On this basis I judged that the RP had undertaken an adequate analysis of the C&I systems against the SEP hazard. I consider it important that ONR engages with the licensee to ensure the measures identified by the RP are implemented as the design develops; the ONR External Hazards inspector has raised Assessment Finding AF-UKHPR1000-0091 for the licensee to address this (Ref. 170).

4.3.2 Strengths

167. The RP has appropriately categorised safety functions and has assigned appropriate classifications to the UK HPR1000 C&I systems.

168. The RP has implemented design modifications to introduce additional diversity and independence in the C&I architecture that will enhance resilience to CCF.

169. The C&I architecture comprises a divisional structure and voting logic to provide resilience against spurious actuation. The RP has undertaken analysis that demonstrates that the C&I architecture provides protection against faults arising from spurious actuation of C&I systems.

170. The RP has undertaken an analysis of the vulnerability of C&I equipment to solar energetic particles and has identified measures to control the hazard.

4.3.3 Outcomes

171. My assessment of the adequacy of the C&I architecture found that the design has adequately considered RGP with regard to the principles of defence-in-depth, independence and diversity. I judged that the RP had provided a suitable and sufficient

demonstration of the independence between C&I systems and con this basis was able to close RO-UKHPR1000-0017 (Ref. 145).

172. I identified four residual matters that have not been resolved within GDA timescales; these are summarised below:

- the RP has not undertaken a comprehensive analysis of the reliability of the UK HPR1000 C&I systems;
- the detailed design of diverse CIM has not been completed in GDA;
- the detailed design of diverse SPM has not been completed in GDA; and
- the RP has not undertaken a comprehensive analysis of the separation and segregation of C&I equipment within the C&I architecture.

173. These matters have been taken forward as Assessment Findings.

4.3.4 Conclusion

174. Based on the outcome of my assessment I have concluded that the C&I architecture has been adequately substantiated for GDA.

175. I identified shortfalls against the expectations of SAPs ERL.1, ERL.2 and ELO.4. I do not judge these shortfalls to be significant enough to prevent the issue of a DAC and I have therefore raised Assessment Findings for them to be addressed by the licensee.

4.4 Examination, Maintenance, Inspection and Testing and Commissioning of C&I systems

4.4.1 Assessment

4.4.1.1 Examination, Inspection, Maintenance and Testing

176. A key regulatory expectation for GDA is that the requirements for EMIT of structures, systems and components important to safety are identified in the safety case. As part of my assessment I sought to understand how EMIT requirements are addressed in the C&I safety case. The key SAPs (Ref. 2) considered in this aspect of my assessment included:

- ECM.1 Commission testing;
- EMT.1 Identification of requirements;
- EMT.2 Frequency;
- EMT.5 Procedures;
- EMT.6 Reliability claims;
- EMT.7 Functional testing; and
- EMT.8 Continuing reliability following events.

177. In GDA Step 3 ONR raised RO-UKHPR1000-0021 (Ref. 40) which identified several shortfalls relating to the consideration of EMIT requirements in the UK HPR1000 safety case. The assessment of the response this RO was led by the Fault Studies specialism and is documented in an assessment note (Ref. 172). I contributed to this assessment, working closely with specialist inspectors from Fault Studies, Mechanical Engineering and Electrical Engineering to assess the submissions. The assessment is not repeated in full in this report, but the aspects relevant to my assessment are summarised in the below paragraphs.

178. I reviewed the ‘EMIT Strategy’ report (Ref. 173) and found that it included the centralised C&I systems within scope of the EMIT safety case; I judged this to be appropriate and that the scope was adequately underpinned.

179. I reviewed the 'EMIT Windows' report (Ref. 174) and found that it identified that there are appropriate windows in which EMIT activities on the C&I systems can be carried out. I then reviewed the 'EMIT Consistency Analysis' (Ref. 175) and noted that the KDS [DAS] and SAS had been screened out of the consistency analysis.

180. The KDS [DAS] had been screened out because the simple-hardware platform is only at the preliminary design stage, and therefore maintenance requirements have yet to be developed. My expectation is that the licensee will develop detailed maintenance requirements for the KDS [DAS], and will demonstrate that these are suitable to support the EMIT strategy. This is addressed as part of AF-UKHPR1000-0030 (see below).

181. The justification for screening the SAS out of the consistency analysis was that because the SAS interfaces with mechanical systems to perform its safety functions, the EMIT strategy for those mechanical systems, in particular periodic testing, will also be applicable to the SAS and hence there is no need for it to be considered separately. I was content with this justification.

182. With respect to the RPS [PS] the consistency analysis (Ref. 175) expands on the 'EMIT Windows' report by identifying suitable windows in which specific EMIT activities can be undertaken, and does not identify any inconsistencies with EMIT requirements.

183. On the basis of the evidence sampled I was content from a C&I perspective that the RP had addressed the expectations of RO-UKHPR1000-0021 and made a recommendation to the Fault Studies specialist inspector that the RO could be closed (Ref. 176).

184. My assessment of the 'BSC of Overall I&C Architecture' (Ref. 44) identified that the CAE did not demonstrate how several relevant SAPs are addressed within the safety case; this included SAPs relevant to EMIT. I raised RQ-UKHPR1000-1447 (Ref. 109) requesting further information to demonstrate how these expectations are met. The RP's response provided a description of where these SAPs are addressed in the BSCs for the individual C&I systems (Ref. 99), (Ref. 100), (Ref. 101), (Ref. 48), (Ref. 49) and (Ref. 102). I sampled the documents and was content that the CAE was sufficient to demonstrate that the SAPs have been adequately addressed.

185. I sampled Revision D of the SRS for the RPS [PS] (Ref. 151) to understand how requirements for EMIT are identified at the system level. I found that the document specified high-level requirements for self-supervision, maintainability and periodic testing. However, there was insufficient information to demonstrate how these requirements had been derived, and how they were considered appropriate for the system.

186. While I am content that the RP has addressed EMIT in the C&I safety case, I consider the lack of detail to be a shortfall against the expectations of SAPs EMT.1 and EMT.5, as the RP has not provided an adequate demonstration that the generic C&I design is suitable to support the EMIT strategy, and that the EMIT requirements are underpinned by the safety case. I consider that these limitations arise because they are related to licensee decisions regarding testing and maintenance during detailed design. I have therefore raised an Assessment Finding for this to be addressed by the licensee.

AF-UKHPR1000-0030 – The licensee shall develop and justify examination, maintenance, inspection and testing arrangements for the UK HPR1000 C&I systems important to safety that reflect the safety case requirements, detailed design of the systems, and licensee choices for test intervals. This should include demonstration that the system architectures are suitable to support the maintenance and testing strategy.

4.4.1.2 Commissioning

187. One of the top-level claims in the C&I safety case (Ref. 3) states that "C&I systems performance will be validated by suitable commissioning and test". My review of the C&I architecture BSC found that the argument supporting this claim referred to the 'Overall C&I Integration Test Plan' (Ref. 177) as the demonstration that procedures for integration testing of C&I systems have been developed. I reviewed this submission and found that, while it provided a high-level description of integration testing activities, it did not provide detailed descriptions of how tests will be carried out. There is therefore insufficient information to demonstrate that the evidence supports the claim.

188. The RP also provided a document defining the strategy for commissioning of C&I systems (Ref. 178). My review of this submission found that it provided high-level details of the commissioning tests that will be carried out on each of the C&I systems, but again did not describe how these tests will be performed. I also noted that the C&I commissioning strategy did not appear to be referenced anywhere in the 'BSC of Overall I&C Architecture' (Ref. 44) – I consider this to be a minor shortfall that will be addressed in the later development phases of the C&I systems.

4.4.2 Strengths

189. The RP has identified appropriate windows in which maintenance and testing of the UK HPR1000 C&I systems can take place and has demonstrated that these windows are consistent with EMIT requirements.

4.4.3 Outcomes

190. My assessment of the examination, maintenance, inspection and testing of C&I systems identified one residual matter, relating to the identification of detailed EMIT requirements, that has not been resolved. This matter has been taken forward as Assessment Finding AF-UKHRP1000-0030.

4.4.4 Conclusion

191. Based on the outcome of my assessment I am satisfied that the consideration of EMIT in the C&I safety case is adequate for GDA. The RP has demonstrated that the UK HPR1000 C&I systems will be subject to regular testing and maintenance, commensurate with their required reliability. On this basis I am content that the expectations of SAPs ECM.1, EMT.2, EMT.6, EMT.7 and EMT.8 have been satisfactorily addressed to the level that would be expected for GDA.

192. I identified shortfalls against the expectations of SAPs EMT.1 and EMT.5. I do not judge these shortfalls to be significant enough to prevent the issue of a DAC and I have therefore raised an Assessment Finding for them to be addressed by the licensee.

4.5 Adequacy of C&I Platforms

193. The RP submissions (e.g. PCSR Chapter 8, (Ref. 3)) state that the UK HPR1000 has four main C&I platforms:

- FirmSys which forms the basis for the Class 1 RPS [PS] and Class 2 SAS.
- Simple Hardware Platform which forms the basis for the Class 2 KDS [DAS].
- HOLLiAS-N which forms the basis for the Class 3 PSAS and KIC [PCICS].
- SpeedyHold which forms the basis for the Class 3 KDA [SA I&C] and auxiliary control panel (ACP).

194. I assessed the suitability of each of the main UK HPR1000 C&I platforms to deliver the reliability and other requirements placed on them by the safety analyses, and the

safety systems that rely on them, considering relevant good practice such as international standards.

195. The outcome of my assessment for each platform is documented in the following sub-sections of my report.

4.5.1 Adequacy of the FirmSys Platform Production Excellence Demonstration

4.5.1.1 Assessment

196. The role of the FirmSys platform is to support the functions performed by the systems that use this platform, namely the RPS [PS] and the SAS, at their required integrity. I note that the RPS [PS] is a Class 1 system, and the SAS is a Class 2 system. My assessment has focused on the claim that FirmSys can meet the Class 1 requirements in performing Category A safety functions, as these are the most onerous, and I have therefore assessed the FirmSys platform PE against the relevant international standards for this, including IEC 61513 (Ref. 21), IEC 60880 (Ref. 16), IEC 60987 (Ref. 17), and IEC 62566 (Ref. 24).

197. I have used SAP ESS.27 (Ref. 2) and NS-TAST-GD-046 (Ref. 10) as the basis for my assessment considering the evidence for Production Excellence (PE) of the FirmSys platform. I assessed the RP's proposals for Independent Confidence Building Measures (ICBMs) that will be used to demonstrate that the PE have been effective separately, and this is reported in Section 4.7.

198. To satisfy the requirements of GDA Step 4, and to remain consistent with previous GDAs, I sought to sample detailed evidence generated by the processes used in the design and development of the FirmSys platform – known as PE. This is important because of the significant claims and arguments made on the FirmSys platform PE ,i.e. Claim C1.1. 1.1, argument A4 "Production Excellence (PE) and Independent Confidence Building Measures (ICBMs) activities are undertaken with a level of rigour suitable for an F-SC1 system", (Ref. 99).

199. The RP produced and submitted three PE summary papers containing partially translated information (Ref. 179), (Ref. 180) and (Ref. 181).

200. I raised several RQ's, namely RQ-UKHPR1000-0930, 0959, 0960, 1000, 1096, 1116, 1117, 1170, 1269, and 1360 (Ref. 109) relating to the adequacy of the evidence provided in these. There were several queries contained within these RQs, which can be broadly summarised around the following themes:

- identification of FirmSys component parts and their classification;
- the use, classification and design of hardware description language programmed devices (HPDs);
- compliance with standards including IEC 60880 (Ref. 16), IEC 60987 (Ref. 17) and IEC 62566 (Ref. 24);
- the scope of the platform verification and validation plan;
- inconsistencies in software processes and procedures; and
- applicability and suitability of the FirmSys PE evidence provided.

201. Having assessed the responses to these RQ's (Ref. 109), combined with my previous assessment of the summary papers, it became evident that there were shortfalls in the PE evidence, but the full nature and extent of these was not clear.

202. To resolve my concerns I raised RO-UKHPR1000-0059 'Evidence of Production Excellence for the FirmSys platform' (Ref. 40), my detailed assessment of which is documented in an assessment note (Ref. 182). This RO had three actions, as follows:

- to review the FirmSys platform PE documentation and identify any shortfalls;

- for each shortfall, to identify compensating measures (CM's) to address this; and
- to develop a strategy for how the CM's would be applied.

203. The RP developed a resolution plan and programme of work (Ref. 183) to respond to the RO, and identified a deliverable, 'Assessment Report of Production Excellence for FirmSys Platform', to communicate the findings. I was content with the proposed resolution plan, and in particular that the RP proposed to use UK TSCs with knowledge of the requirements and application of the relevant international standards in a UK regulatory context. The deliverable was submitted to ONR with revision A (Ref. 184) to report PE shortfalls that had been identified, and revision B (Ref. 185) to also report any identified CMs and programme to deploy these.

204. I assessed revision A (Ref. 184) and raised RQ-UKHPR1000-1698 (Ref. 109) to query apparent discrepancies between the assessment outcomes and the requirements of the standards clauses. The response to RQ-UKHPR1000-1698 (Ref. 109) provided, for each item, an explanation as to how a particular discrepancy had arisen and how it had already been addressed in revision A of the report, or further information on how this would be addressed in revision B of the report. This response gave me confidence that the discrepancies I had identified would be resolved in revision B of the report.

205. I assessed the final revision (revision B) of 'Assessment Report of Production Excellence for FirmSys Platform' (Ref. 185). My findings are recorded in my RO closure note (Ref. 182) and are summarised below:

- The RP has undertaken a review of the FirmSys platform PE documentation during GDA Step 4 and has identified shortfalls in the evidence.
- The RP has identified at least one CM for each shortfall identified.
- The RP has developed a strategy and indicative programme for how the CMs would be applied.

206. I concluded that the actions had been broadly satisfied and that it was appropriate to close the RO.

207. The submission 'Assessment Report of Production Excellence for FirmSys Platform', Revision B (Ref. 185) identified gaps in the FirmSys platform PE evidence against international standards clauses, and grouped and summarised these into shortfalls in the following areas:

- Overall development approach and quality assurance (QA) processes (e.g. completeness, consistency and clarity of requirements specifications; lack of detail in verification records; software tool selection and justification, etc.).
- Hardware development gaps (e.g. hardware design specification; hardware verification; revalidation required after maintenance .etc.).
- Software development gaps (e.g. software design documentation; testing and simulation of behaviour of executable code; software modularity and complexity .etc.).
- Hardware description language (HDL) - programmed devices (HPD's) development gaps (e.g. software design documentation; testing and simulation of behaviour of executable code; software modularity and complexity .etc.).
- Documented nuclear safety and security design principles and guidelines. (note: the assessment of cyber security of C&I systems is documented in Section 4.8)

208. My observations on the suitability of the approach used by the RP to identify FirmSys PE evidence shortfalls, and in decision-making, are summarised below.

- The work reviewed a suitable sample of PE evidence, comprising many individual evidence documents. The approach to sentencing anomalies by a diverse review group appears to have been effective at identifying and classifying both adequate and inadequate PE evidence. Whilst many clauses of relevant international standards appear to have been met by the evidence reviewed, a significant number of shortfalls against the requirements of international standards were identified (see above).

- A significant number of standards clauses were reported to be not applicable (N/A). However, it was not clearly recorded in some cases exactly why, and in other cases the clauses did appear to be applicable. For example, IEC 60880 clause 6.1.8 “Special operating conditions such as plant commissioning and refuelling shall be described down to the software level for the functions that are impacted.” was recorded as N/A with the comment “Operating modes of the plant are not in scope for the assessment”. However, I note that the FirmSys platform needs to be able to support a range of operating conditions, such as changing parameters, proof test and maintenance. It is my opinion the omission of these requirements in the assessment is inappropriate and represents a shortfall in the scope of the assessment. I judge that the selection of N/A in this case to be inappropriate, and I consider it likely that similar limitations may exist for other standards clauses. My conclusion is that the RP has not provided sufficient justification for the non-applicability of clauses that have been identified as N/A. I consider this to be a shortfall that should be addressed by the licensee and has therefore been included in AF-UKHPR1000-0031 (see below).

- My sampling of the standards clauses which were documented as “OK” in the report identified clauses which, in my opinion, had not been adequately addressed by the evidence cited, or for which the outcome did not match the evidence cited. For example, clause 6.2.3 of IEC 60880 states “The self-supervision should be able to detect to the extent practicable: random failure of hardware components, erroneous behaviour of software (e.g. deviations from specified software processing and operating conditions or data corruption), and erroneous data transmission between different processing units”. The report indicates this clause has been met (i.e. “OK”), yet the commentary states “The FMEA only consider the hardware failure. There are no related information about software.” and “An FMEA for communication faults is documented in Section 2.3 of [048]. A number of potential communication issues are assessed with the checks/mitigations in place described. However, we do not know how these formally link to design requirements or tests from this report.”. This commentary contradicted the RP’s conclusion that the clause had been met, which undermines my confidence in the outcomes of the assessment. I judge the potential consequences of this finding to be significant, as the programme to resolve the identified gaps in the FirmSys PE is already a significant one, and I consider that additional work will be required to resolve gaps that have not been identified. In addition it is my opinion that the gap I have cited would require both software faults and erroneous data transmission to be considered, and if not adequately done at the design stage then this could lead to design changes being required at a later stage in development. In my opinion this has the potential to undermine the feasibility of the RP’s programme, as outlines in (Ref. 185). I have therefore included this point in AF-UKHPR1000-0031 (see below).

- The standards considered in the assessment and documented in the report (i.e. IEC 61513, IEC 60880, IEC 62566, and IEC 60987) are all top tier nuclear power plant standards that refer to normative standards that are “…indispensable for the application of this document [the standard]”. For

example, IEC 61513 cites IEC 61500 (Nuclear power plants – Instrumentation and control important to safety – Data communication in systems performing Category A functions) (Ref. 19)among others as a normative standard. A complete demonstration of FirmSys platform PE will need to consider all requirements of all relevant standards that apply, unless it can be shown that these are not applicable, or that an equivalent approach has been applied and is adequate. I am of the opinion that this should be addressed by the licensee as part of detailed design and substantiation of these systems and therefore I have included this point in AF-UKHPR1000-0031 (see below).

209. My observations of the FirmSys platform PE evidence shortfalls and CMs identified by the RP are:

- Some shortfalls are particularly significant and far reaching in their potential impact on the FirmSys platform design. For example, the lack of high-level nuclear safety design principles and guidelines has the potential to affect all design and verification activities, because it is currently not clearly documented what the design objectives are and therefore what the impact of shortfalls will be on overall risk control. Similarly, the lack of completeness, consistency and clarity of requirements specifications, and traceability of requirements through the development means that it difficult to confirm the design meets its intent, and that it is not possible to demonstrate the FirmSys platform design is able to adequately control risk.

- The shortfalls relate to a wide range of safety lifecycle stages. I observe that many lifecycle stages result in iterative design activities being necessary where limitations in the design against its objectives are identified and design activities need to be repeated to address these. The programme of work set out to resolve the identified shortfalls is largely linear, and the resourcing estimates reflect a once-through approach. However, iterative work may be necessary to resolve the shortfalls, and this may result in additional resources being required to address a particular shortfall.

- The RP has assessed the suitability of CMs to resolve the shortfalls identified by checking that each proposed CM meets the requirements of all the standards clauses associated with the shortfall. Whilst the RP has confirmed that the CMs identified address all relevant clauses, I note that this does not mean that this will result in a coherent and comprehensive design process that ensures the design meets all the safety objectives. Furthermore, it is not possible to determine whether the safety objectives will be met by the proposed CMs because one of the identified shortfalls is the lack of higher level objectives.

210. The RP has developed a programme of work to address the shortfalls identified using CMs, and this is documented in ‘Assessment Report of Production Excellence for FirmSys Platform’, Rev. B (Ref. 185). This programme of work is substantial, with many thousands of person days of effort required. The RP has stated that it is feasible for this work to be accomplished during the reactor build programme and provided some evidence to support this assertion in the report.

211. I identified limitations in the proposed approach in a number of areas, including the potential for further shortfalls to be identified once work is underway, the difficulty in accurately estimating resource requirements, the potential for later stages of the programme to result in re-work of earlier stages, and the potential for this work to become focused on meeting the requirements of standards clauses rather than establishing a top-down safety lifecycle that adequately identifies, manages, and demonstrates control of risks. I therefore raised RQ-UKHPR1000-1747 (Ref. 109) to

request more information in the area of competence, and RQ-UKHPR1000-1756 (Ref. 109) seeking further justification of the conclusions, sequencing of compensating activities, hazards management, extent of potential design modifications, design lifecycle and safety case, and the suitability of proposed oversight arrangements.

212. I was satisfied with the responses to RQ-UKHPR1000-1747 (Ref. 109) in that these provided me with confidence that suitable competence arrangements would be put in place, in particular that external support with expertise in the relevant international standards would be utilised, and that competence arrangements would be baselined against a recognised safety skills framework such as the IET code of practice: 'Competence for Safety Related Systems Practitioners' (Ref. 186).

213. I reviewed the responses to RQ-UKHPR1000-1756 (Ref. 109) and was generally satisfied that:

- the sequencing of CMs appears appropriate and can be substantiated;
- hazards will be managed by the development of a CAE tree to demonstrate that a coherent design has been achieved that adequately controls risk;
- criteria for establishing the need for design modifications will be established;
- the design lifecycle will be developed to align with RGP and a safety case will be established; and
- oversight arrangements will include an external oversight group chaired by the licensee.

214. However, the response to RQ-UKHPR1000-1756 query 1 (Ref. 109) states that "In fact, there is evidence that the platform is indeed suitable [for Class 1 applications], as it is currently being used in several nuclear power plants and no issues have so far been identified.". I judge this statement does not adequately consider the failure causes in complex C&I systems, or what evidence is required to underpin such a claim, particularly for a demand-mode system designed to achieve a high safety integrity. Furthermore, the FirmSys documentation sampled in GDA makes no reference to this claim and it is therefore not clear what relevance it has to the safety case. My expectation is that the justification of the Class 1 FirmSys platform will be primarily based on deterministic and analysis approaches, as per the expectations of SAP ESS.27.

215. Taking the points identified above, I have raised the following Assessment Finding in relation to the PE aspects of the FirmSys safety case, noting that similar shortfalls have also been identified for other platforms and systems.

AF-UKHPR1000-0031 – The licensee shall develop production excellence evidence for the detailed design of the FirmSys platform, to justify that FirmSys is suitable to form the basis of the UK HPR1000 Reactor Protection System and Safety Automation System. This shall comprise, as a minimum, the following activities, or equivalent:

- define the scope of production excellence evidence necessary to support the safety case, and how this will be presented in a way that facilitates independent oversight;
- consideration of the safety objectives of the platforms and systems, and the need to implement measures to control the effects on system operation of internal failures and faults;
- revisit the self-assessment and compensating strategy developed during GDA, demonstrating that all of the gaps in the FirmSys platform have been identified, along with means to address those gaps;
- validate the schedule developed in GDA, including any changes necessary to resolve this finding, making allowance for enhanced regulatory oversight to be provided; and

- demonstrate that the organisational capability and capacity required for development of the FirmSys platform for the UK HPR1000, including that required to maintain independent oversight, can be maintained throughout the programme of work.

4.5.1.2 Strengths

216. During GDA Step 4 the RP initiated an independent review of the FirmSys PE documentation which identified a number of shortfalls, and developed a programme of work to undertake CMs that will address these shortfalls.

4.5.1.3 Outcomes

217. The finding of my assessment is that the FirmSys platform PE documentation is inadequate to demonstrate that the FirmSys platform is suitable to form the basis for the RPS [PS] and SAS. The number and significance of the shortfalls identified by an independent review during GDA Step 4, and reported in (Ref. 185) are such that significant work will be required to resolve those shortfalls identified, and during GDA the RP put forward an extensive programme work to resolve this matter that can be implemented by a licensee. Furthermore, it is my opinion that further shortfalls may be identified as work progresses. This has been taken forward as Assessment Finding AF-UKHPR1000-0031. However, the RP's assessment of the FirmSys PE, and the programme of work for resolution of the identified shortfalls, was sufficient to enable me to close RO-UKHPR1000-0059 (Ref. 182).

4.5.1.4 Conclusion

218. It is my opinion that the shortfalls identified by the RP in the FirmSys platform PE evidence are significant, and that SAP ESS.27 and TAG NS-TAST-GD-046 have not been satisfied. The safety case claim and argument (C1.1. 1.1, argument A4) that "Production Excellence (PE) and Independent Confidence Building Measures (ICBMs) activities are undertaken with a level of rigour suitable for an F-SC1 system" has not been substantiated, and therefore the FirmSys platform has not been demonstrated to be suitable to form the basis for the RPS [PS] and SAS at the end of GDA Step 4. I have raised AF-UKHPR1000-0031 (see above) for these shortfalls to be addressed during detailed design of the RPS [PS] and SAS by the licensee.

4.5.2 Adequacy of the Simple Hardware Platform

4.5.2.1 Assessment

219. In GDA Step 2 (Ref. 187) ONR raised RO-UKHPR1000-0001 'Diverse Actuation System Design Shortfalls' (Ref. 40) which highlighted the following shortfalls in the design of the KDS [DAS] against UK regulatory expectations:

- The system was designed in accordance with Class 3 despite being responsible for the delivery of Category B safety functions.
- The platform was based on complex programmable hardware, therefore compromising the argument of diversity between the RPS [PS] and the KDS [DAS].
- The system was not designed to meet the single failure criterion, meaning it could be rendered inoperable by the failure of a single component.

220. During GDA Steps 3 and 4 I undertook assessment of the RP's submissions in response to RO-UKHPR1000-0001. The detailed assessment is documented in an assessment note (Ref. 188) and is not repeated in full here. The key points of my

assessment are summarised in the following paragraphs. The SAPs (Ref. 2) that informed my assessment of the simple hardware platform included:

- EKP.2 Fault tolerance;
- ECS.2 Classification of structures, systems and components;
- ECS.3 Codes and standards;
- EQU.1 Qualification procedures;
- EDR.3 Common cause failure;
- EDR.4 Single failure criterion;
- ERL.2 Measures to achieve reliability;
- ESS.1 Provision of safety systems; and
- ESS.18 Failure independence.

221. The RP provided a document titled 'Safety Requirements of the KDS [DAS]' (Ref. 189) which specified the safety requirements to be achieved by the system. My review of this submission found that the RP had revised the classification of the KDS [DAS] to Class 2 on the basis that it provides a diverse backup to the RPS [PS] and is the principal means of delivering Category B safety functions.

222. I also found that the document specified requirements that would address key safety principles including independence, diversity, redundancy, segregation and reliability, as well as requirements for qualification, diagnostics, testing and maintenance. These requirements are fulfilled at the system level rather than the platform level and therefore my assessment is detailed further in sub-section 4.6.3 of this report.

223. To address concerns raised in RO-UKHPR1000-0001 (Ref. 40) the RP undertook research into the implementation technology for the KDS [DAS] (Ref. 190) which concluded that the preferred solution was the development of a dedicated 'simple hardware-based platform' for the KDS [DAS], and presented a preliminary design scheme for the platform. While I was content with this conclusion, I noted that the platform in fact incorporated programmable components in the form of dedicated cards to perform monitoring and test functions. Though those are not claimed in delivery of safety functions I was concerned about the potential for programmable components to interfere with safety functions and present a risk that common cause failures could simultaneously affect multiple C&I systems important to safety.

224. I therefore raised RQ-UKHPR1000-0512 (Ref. 109) asking the RP to justify its position. In its response the RP committed to provide a FMEA for the KDS [DAS] during GDA Step 4 to demonstrate that programmable elements cannot compromise delivery of safety functions.

225. I reviewed the FMEA (Ref. 97) and found that it did not provide a suitable and sufficient justification that failure of the programmable electronics could not interfere with the safety functions. I therefore raised RQ-UKHPR1000-1144 (Ref. 109) seeking additional information. In response the RP provided a further document, 'Justification for the Non-interference of Safety Functions in KDS [DAS]' (Ref. 98). The findings of my review of this document are summarised in the following paragraphs.

226. The document provides a description of the architecture of the simple hardware-based platform, including simple schematics showing how the programmable cards are isolated from the processing hardware. It also shows that the self-diagnostic features of the simple hardware-platform are implemented in hardware and are independent of the monitoring and test cards.

227. The document sets out environmental qualification tests that will be performed for the simple hardware-based platform and confirms that the programmable components will be qualified to the same level as the hardware components, to ensure resilience to hazards.

228. The document provides a high-level failure modes analysis of the monitoring and test cards, using representative data from a FMEA of similar components (in terms of function blocks and architecture) from the FirmSys platform. This demonstrates that failure of the monitoring and test cards will be revealed and will not impact on delivery of the KDS [DAS] safety functions.

229. My assessment of the RP's approach to FMEA and reliability analysis is detailed in Section 4.3 of this report. It is my expectation that, as the design of the simple hardware platform develops, further detailed analysis of the platform hardware will be undertaken – this is captured as part of Assessment Finding AF-UKHPR1000-0026 (see Section 4.3).

230. I was content that the RP had provided a suitable justification that the diversity of the KDS [DAS] is not compromised, and I judged the level of detailed information provided to be commensurate with what would be expected at the preliminary design stage. Note that because the programmable cards play no part in the delivery of safety functions, I have not undertaken an assessment against the expectations of SAP ESS.27.

231. In GDA Step 4 the RP also provided a development plan (Ref. 191) and a qualification plan (Ref. 192) for the simple hardware platform, setting out respectively the activities that will be undertaken through the development lifecycle and the qualification tests that will be performed to demonstrate that the equipment can meet its environmental performance requirements.

232. I reviewed the development plan (Ref. 191) and found that it provided insufficient information to give confidence that the platform would be developed according to a structured lifecycle. In particular I noted that there was no information to demonstrate the independence and diversity of the development team from teams involved in the development of other platforms and systems used in the UK HPR1000. There was also no information regarding the quality management processes and procedures that will be in place to manage the development. I therefore raised RQ-UKHPR1000-1087 (Ref. 109) to seek further clarification on these issues.

233. The RP provided its response to this RQ, along with a revised version of the development plan (Ref. 193). I reviewed this submission and found that some of my queries had been adequately addressed; in particular a full description was provided of the organisational arrangements that will be in place to ensure independence and diversity between development teams will be achieved. This gave me sufficient confidence that this potential source of systematic faults will be adequately controlled. However, several of my queries had not been satisfactorily resolved and I therefore raised RQ-UKHPR1000-1566 (Ref. 109) as a follow up.

234. The response to this RQ, along with a further revision of the development plan (Ref. 194) provided significantly more information to describe how the development lifecycle will be managed, including references to overarching quality management procedures and how the lifecycle aligns with RGP from international standards, in particular IEC 61513 (Ref. 21), IEC 60987 (Ref. 17) and IEC 61508 (Ref. 20). Having reviewed these submissions I was content that the RP had established an adequate plan for managing the development lifecycle of the Simple Hardware Platform.

235. My review of the 'Equipment Qualification Plan for the Simple Hardware-based Platform' (Ref. 192) found that it was unclear as to how it had considered international standards that ONR judges to be RGP, in particular IEC 60780 (Ref. 15). I therefore raised RQ-UKHPR1000-1118 (Ref. 109) asking the RP to provide further clarification as to how the qualification plan addresses that standard.

236. The RP's response further described how the qualification plan has considered the expectations of RGP. A revised version the qualification plan was also submitted (Ref. 195), which provided significantly more information to demonstrate how the qualification tests will meet the requirements of international standards. Having reviewed these submissions I was content that my queries had been satisfactorily resolved and that the RP has established an adequate plan for the environmental qualification of the simple hardware platform.

237. Based on the evidence sampled in my assessment of the simple hardware platform I have concluded that the RP has provided adequate justification that, at the platform level, diversity between the KDS [DAS] and other C&I systems will be achieved, and that the preliminary design presented meets regulatory expectations for GDA. I judge that the documentation provided to describe the development and qualification plans demonstrate that a suitable design lifecycle is in place, that appropriate standards have been considered and that a suitable platform is available to support the UK HPR1000 C&I architecture.

4.5.2.2 Strengths

238. The RP has provided adequate justification that, at the platform level, diversity between the KDS [DAS] and other C&I systems will be achieved, and has demonstrated that a suitable design lifecycle is in place.

4.5.2.3 Outcomes

239. My assessment of the adequacy of the Simple Hardware Platform found that the platform is suitable to form the basis of the KDS [DAS] for the UK HPR1000, and that there is a plan to ensure that adequate diversity is maintained throughout the development lifecycle. Based on the submissions provided I judged that the RP had provided sufficient evidence to enable RO-UKHPR1000-0001 to be closed (Ref. 188).

4.5.2.4 Conclusion

240. Based on the outcomes of my assessment I am of the opinion that the RP has provided an adequate justification for the simple hardware platform in the context of GDA. The implementation technology is sufficiently diverse from the computer-based RPS [PS] and the development and qualification of the platform will follow a structured lifecycle that is aligned with international standards. On this basis I am content that, for the simple hardware platform, the RP has satisfactorily addressed the expectations of SAPs EKP.2, EKP.3, ECS.2, ECS.3, EQU.1, EDR.3, EDR.4, ERL.2, ESS.1 and ESS.18.

4.5.3 Adequacy of the HOLLiAS-N Platform

4.5.3.1 Assessment

241. I have used SAP ESS.27 and NS-TAST-GD-046 as the basis for my assessment, considering the evidence for Production Excellence (PE) of the HOLLiAS-N platform. I assessed the Independent Confidence Building Measures (ICBMs) that will be used to demonstrate that the PE have been effective separately, and this is reported in Section 4.7.

242. The RP submitted a number of documents to relevant to the HOLLiAS-N platform, including:

- 'Topic Report of HOLLiAS-N Platform' (Ref. 196).
- 'HOLLiAS-N Platform Compliance Analysis with IEC 62138' (Ref. 85).
- 'Demonstration of Production Excellence for HOLLiAS-N' (Ref. 75).

243. The HOLLiAS-N platform forms the basis for the Class 3 PSAS and KIC [PCICS] systems. Safety case claims for the PSAS and KIC [PCICS] are documented in the 'BSC of Plant Standard Automation System (Ref. 48)' and 'BSC of Plant Computer Information Control System' (Ref. 49). The PSAS and KIC [PCICS] perform FC3 (Category C) safety functions. Their reliability targets are set at 10^{-1} failures per year in continuous mode operation (Ref. 44). The HOLLiAS-N platform inherits this reliability claim.

244. In assessing the HOLLiAS-N platform, I sampled the form of the claims, arguments and evidence presented, sufficient to develop suitable conclusions.

245. The submission 'Topic Report of HOLLiAS-N platform' (Ref. 196) provides an overview of the HOLLiAS-N platform components and design processes, software verification and validation, and equipment validation. This document provides some information, such as a high-level mean time between failures (MTBF) calculation, but I found the submission is structured to document the design rather than provide a case for its adequacy, and there is insufficient detail to provide a convincing argument, or to substantiate the claims made.

246. The submission HOLLiAS-N platform compliance analysis with IEC 62138 (Ref. 85) reports how the HOLLiAS-N platform meets the clauses of IEC 62138. My assessment found that the relevant clauses of IEC 62138 have been identified, and that individual points in those clauses have been separated out, so they can be responded to specifically. I consider this good practice.

247. I observe that IEC 62138 states that for Class 3 systems it is necessary show that the software "contributes as necessary to, and does not adversely affect, the functions important to Safety", and "satisfies the Software Requirements Specification statements which define constraints important to safety".

248. My assessment of the documented responses to the clauses in IEC 62138 (Ref. 85) considered whether this had been achieved for this Class 3 system. I found that some clause compliance statements did not provide sufficient information to demonstrate that this objective has been met. For example, clause 5.1.4, 1 "Software tools should support the development activities which contribute to the correctness of software and system design." elicits the following analysis "The following software tools are widely used software development tools and are suitable for the development of HOLLiAS-N system software: a) Software development tools: VC++6.0, C, VBA; b) Embedded development tools: KEIL uVision4, Xilinx ISE 12.4, Quartus II 9.1, Code Warrior 5.9.0, CCS 3.3, PADS 9.0, ModelSim 10.5;.". Specifically, this does not state how the selected tools support the development activities which contribute to the correctness of the software and system design, or provide evidence that they are effective. In addition, there is no reference to the software requirements specification, and whether the safety constraints have been satisfied by the tools selected.

249. The report concludes that "No gaps or weaknesses are identified in the comparison analysis, so the design of UK HPR1000 RPS [PS] is consistent with the requirements defined in IEC 62138". I cannot concur with this conclusion as it is my opinion that insufficient information has been provided to support the safety case claims. Considering the low safety significance of the systems that use the HOLLiAS-N platform, I do not consider that it is necessary for this to be addressed during GDA. However, I am of the opinion that confirmation that the requirements of this standard have been satisfied will be necessary so that the HOLLiAS-N platform design can be substantiated during the detailed design and substantiation of the PSAS and KIC [PCICS]. This is addressed by AF-UKHPR1000-0033 (see below).

250. The submission 'Demonstration of Production Excellence for HOLLiAS-N' (Ref. 75) provides a brief description of the HOLLiAS-N platform components, its development

process, quality management, and lists the operational experience of systems using the HOLLiAS-N platform. I considered the overall approach to the demonstration of the HOLLiAS-N PE, and then separately the evidence to support the claims on the development and quality management processes, and the significance of the cited operational experience.

251. My assessment identified that there are three arguments relating to HOLLiAS-N PE:

- Argument 1 – "The development process of the HOLLiAS-N platform complied with the relevant standards and applied a comprehensive V&V programme to check every system function".
- Argument 2 – "The development process of the HOLLiAS-N platform implemented a modern standard quality management system".
- Argument 3 – "The HOLLiAS-N platform has been successfully applied to multiple engineering projects and obtained international authoritative third-party certifications".

252. The structure of the safety case is appropriate, with sub arguments and evidence uniquely identified. I observed that the safety case is organised according to the design lifecycle phases, e.g. the platform hardware requirements specification phase, hardware detailed design phase, etc. It is my opinion that whilst this is able to present the evidence associated with each lifecycle phase, it does not necessarily confirm that all the activities together produce a platform that is suitable for the claimed classification. Nevertheless, the case is adequately detailed, and evidence is presented to support the arguments made.

253. The sub arguments presented are adequately detailed in most cases, clearly describing inputs and outputs of each phase, and the activities within it. I noted that high-level QA activities are included in the sub arguments, e.g. peer review, and that specific evidence documents are referenced. However, in some cases the evidence documents cited do not appear to match the evidence described in the argument, or are not referenced. For example, I noted that the evaluation of the whether the field programmable gate array (FPGA) design meets the functional and performance requirements is recorded in the programmable logic design evaluation record, but no programmable logic design evaluation record is cited as evidence, only specification documents.

254. I judged that some of the sub arguments are difficult to comply with. For example, in the software realisation phase it is stated that "The criterion of passing the software unit test is: statement coverage is 100%, C/DC coverage is 100%, and MC/DC coverage is 100%.". Based on the description of the HOLLiAS-N platform, it appears diagnostic and defensive software code is incorporated to detect hardware failures, software faults or communication errors, so that consequences of these events can be managed. I note that this code is difficult to fully test because it is often challenging to place the system into a state which allows this. Therefore I judge that the RP has not provided is sufficient evidence to support this claim. Whilst I do not consider it appropriate to resolve this issue during GDA, I consider that the lack demonstration of the validity and appropriateness of the claims is a shortfall that should be resolved during the detailed design and substantiation of the C&I systems. This is included as part of Assessment Finding AF-UKHPR1000-0033 (see below).

255. In addition to the points above I noted a number of other anomalies in the 'Demonstration of Production Excellence for HOLLiAS-N' (Ref. 75). This includes apparent gaps in the lifecycle phases (e.g. overall operation and maintenance), apparent lack of completeness of the systems requirements activity, lack of detail (e.g. hardware realisation unit test description does not state how the tests are adequate), lack of reference to procedures (e.g. software realisation phase V&V procedure), and lack of information on the HOLLiAS-N platform periodic test requirements.

256. I identified a number of apparent anomalies regarding the HOLLiAS-N PE demonstration, and note that identification and confirmation of the suitability of the evidence to support the arguments will be necessary during lite-specific stages.

257. I consider this to be of sufficient importance for it to be tracked to closure and I have therefore raised an Assessment Finding for this to be addressed by the licensee:

> AF-UKHPR1000-0033 – The licensee shall demonstrate the production excellence of the HOLLiAS-N and SpeedyHold platforms for the UK HPR1000, using an equivalent methodology to that applied to the Class 1 FirmSys platform during GDA. This shall give particular consideration to the following, as a minimum:
>
> - the identified safety objectives of the platform and systems;
> - the need to implement measures to control the effects on system operation of internal failures and faults; and
> - the validity and appropriateness of the claims, including those related to testing and test coverage.

4.5.3.2 Strengths

258. My assessment found that the structure of the safety case relating to the HOLLiAS-N platform is suitable to support further development. My expectation is that the safety case will be further developed by the inclusion of the necessary evidence to underpin the adequacy of the HOLLiAS-N platform during the detailed design and substantiation of the systems it supports.

4.5.3.3 Outcomes

259. My assessment of the HOLLiAS-N platform found that an appropriate safety case structure has been established and that claims are supported by appropriate arguments. However, these arguments will need to be underpinned by suitable evidence during detailed design and substantiation. I found gaps in some evidence cited within the safety case, and also that at least one argument will be difficult to comply with (that software is 100% tested). My expectation is that these issues will be addressed by the licensee and have therefore raised Assessment Finding AF-UKHPR1000-0033 for them to be taken forward.

4.5.3.4 Conclusion

260. Based on the evidence sampled I judge that the HOLLiAS-N platform has not been demonstrated to be suitable to form the basis of the PSAS and KIC [PCICS] systems at the end of GDA Step 4. I have raised AF-UKHPR1000-0033 for this to be addressed by the licensee.

4.5.4 Adequacy of the SpeedyHold Platform

4.5.4.1 Assessment

261. I have used SAP ESS.27 and NS-TAST-GD-046 as the basis for my assessment, considering the evidence for Production Excellence (PE) of the SpeedyHold platform. I assessed the Independent Confidence Building Measures (ICBMs) that will be used to demonstrate that the PE have been effective separately, and this has been reported in Section 4.7.

262. The RP submitted a number of documents relevant to the SpeedyHold platform, including:

- ‘BSC of Severe Accident I&C System’ (Ref. 102).

- ‘KDA [SA I&C] System Requirements Specification’ (Ref. 63).
- ‘Topic Report of SpeedyHold Platform’ (Ref. 197).
- ‘Suitability Analysis Report of the Selected Platform Applicability to the KDA [SA I&C] System Requirements’ (Ref. 198).
- ‘Product Excellence Summary Paper for Algorithm Calculation and Power Failure Protection Function of SpeedyHold’ (Ref. 199).

263. The SpeedyHold platform is used to implement the KDA [SA I&C] system. Safety case claims for the system are documented in the ‘BSC for the KDA [SA I&C] System’ (Ref. 102). The reliability claim for the KDA [SA I&C] is 10^{-1} pfd and the system performs FC3 (Category C) safety functions.

264. The ‘KDA [SA I&C] System Requirements Specification’ (Ref. 63), requirement [KDA-SRS-0001] sets the requirement that the KDA [SA I&C] system is an F-SC3 (Class 3) system. The SpeedyHold platform inherits this claim.

265. I observe that there are some claims that appear incompatible with the claimed reliability of the SpeedyHold platform, such as [KDA-SRS-0220] which states “The probability of spurious actuation for the function of manual opening of the passive reactor pit injection shall be lower than 10-7 /year.”. However, I note that during GDA Step 4 the design of this function has been changed so that it is hardwired and cannot be influenced by the SpeedyHold platform. This, and other modifications are documented in the KDA [SA I&C] BSC (Ref. 102) and discussed further in sub-section 427.

266. The ‘Topic Report of SpeedyHold platform’ (Ref. 197) provides an overview of the SpeedyHold platform components, quality assurance system and processes, lifecycle and development processes, and equipment qualification approaches. This document provides some information, such as that relating to environmental tests, but it is structured to document the design rather than develop a case for its adequacy. I also noted that there is insufficient detail to substantiate that the SpeedyHold platform meets the requirements of relevant international standards, such as IEC 62138 (Ref. 22).

267. I assessed the ‘Suitability Analysis Report of the Selected Platform Applicability to the KDA [SA I&C] System Requirements’ (Ref. 198). This sets out information relating to SpeedyHold, including the codes and standards applicable to the platform, its architecture, the quality assurance programme applied to it, development lifecycle, qualification, and performance requirements. The section on performance analysis cites some relevant requirements, such as [SRS-0051] on the probability of failure on demand of the KDA [SA I&C] system. This does not reference evidence that this requirement can be achieved by the SpeedyHold platform, but simply states “Satisfy”. Similarly, no evidence is referenced to support the assertion that the SpeedyHold platform can support a time delay between a change in parameter and indication on the SHP or KIC [PCICS] of no more than 1.5 seconds. Other requirements such as the frequency of spurious actuation of the passive pit injection [KDA-SRS-0220] are not referenced at all, so there is no information provided as to whether the SpeedyHold platform is capable of supporting this requirement. I observe that out of over 200 requirements, only 12 are considered in this document. It is therefore my judgement that this document is not adequate to demonstrate that the SpeedyHold platform is suitable to support the requirements of the KDA [SA I&C] system. I consider this issue to be of sufficient significance that this should be tracked to completion through AF-UKHPR1000-0033.

268. I noted a number of anomalies in the ‘Demonstration of Production Excellence for SpeedyHold’ (Ref. 77). These are similar in nature to the shortfalls identified with the FirmSys and HOLLiAS-N platforms. I note that the justification of the suitability of the SpeedyHold platform will need to be completed during detailed design and

substantiation of the C&I systems. I have therefore included this as part of Assessment Finding AF-UKHPR1000-0033.

4.5.4.2 Strengths

269. The RP responded to my concerns regarding the limitations to the demonstration of adequacy of the SpeedyHold platform, and whilst further work is required during the detailed design and substantiation of the system, modification M89 (Ref. 200) was implemented to the KDA [SA I&C] system. This is to reduce the potential for a fault with the SpeedyHold platform to prevent the severe accident displays and controls from operating correctly.

4.5.4.3 Outcomes

270. I identified a number of shortfalls regarding the SpeedyHold platform during GDA Step 4, including a lack of clarity and traceability of system requirements, and evidence that the requirements of relevant standards has been satisfied by the design. These shortfalls are similar to that observed for the other platforms and are addressed by AF-UKHPR1000-0033. I note that the modification to the KDA [SA I&C] system significantly reduces its dependence on the correct operation of the SpeedyHold platform. However, I am of the opinion that the RP has not fully identified the consequences of incorrect operation of the SpeedyHold platform and that this should be addressed as the detailed requirements of the KDA [SAS I&C] system are established during detailed design. This is discussed further in sub-section 427.

4.5.4.4 Conclusion

271. I conclude that sufficient progress has been made during GDA to establish an outline safety case for the SpeedyHold platform, and to identify further work to be accomplished during site-specific stages of the project. Based on the evidence sampled I judge that the SpeedyHold platform has not been demonstrated to be suitable to form the basis of the KDA [SA I&C] system at the end of GDA Step 4. I have raised AF-UKHPR1000-0033 for this to be addressed by the licensee.

4.6 Adequacy of C&I Systems

272. My assessment of the adequacy of the UKHPR1000 C&I systems has considered the centralised C&I systems, namely:

- The Class 1 RPS [PS].
- The Class 2 SAS.
- The Class 2 KDS [DAS].
- The Class 3 PSAS.
- The Class 3 KIC [PCICS].
- The Class 3 KDA [SA I&C].

273. For the UKHPR1000 centralised C&I systems within scope of GDA, I identified areas of interest regarding the suitability of the system designs, including:

- the adequacy of the substantiation of safety functional claims;
- the approach to the design and substantiation of system components in respect of relevant international standards and ONR's expectations;
- the suitability of the system design to achieve the required safety properties;
- appropriate use of technology and it's application, including dedication to a single task;
- avoidance of influence of higher-class systems from lower-class systems;
- the suitability of the approach to testing and maintenance;

- the approach to configuration control of application software and parameters; and
- measures are in place to avoid spurious actuation of the systems.

274. The outcome of my assessment for each system is presented in the following sub-sections.

4.6.1 Adequacy of the RPS [PS]

4.6.1.1 Assessment

275. The 'BSC of Protection System' (Ref. 99) contains claims that the protection system performs a range of FC1 (Category A) safety functions such as reactor trip and cooling functions to directly maintain reactor safety in the event of a loss of control of the plant control and other relevant systems. I assessed the RPS [PS] on the basis that this is a Class F-SC1 (Class 1) system performing FC1 (category A) safety functions. The RPS [PS] is implemented using the FirmSys platform.

System Requirements

276. I sought to confirm that the adequate system requirements have been identified for the RPS [PS]. My assessment considered a range of SAPs including ESS.10 and ESS.11 relating to capability and adequacy, as well as IEC 61513 (Ref. 21), and was informed by relevant RP submissions, including:

- 'BSC of Protection System' (Revision F) (Ref. 99).
- 'UK HPR1000 Fault Schedule' (Revision D) (Ref. 131).
- 'RPS [PS] System Requirements Specification' (Revision D) (Ref. 151).

277. My assessment identified that it was difficult to trace some requirements from the 'BSC of Protection System' (Ref. 99) to the RPS [PS] system requirements specification (Ref. 151) because requirements were named differently between these two documents. I raised RQ-UKHPR1000-1008 (Ref. 109) requesting clarification on the specific functions identified but also more generally how it is shown the system requirements are complete and unambiguous. The response to this RQ claimed that all requirements in the BSC could be traced to the SRS, and that the SRS covers all the functions defined in the BSC but acknowledged that discrepancies exist between these two documents and that this arises from the upstream definition and naming of functions.

278. My assessment also identified that it was difficult to trace some requirements from the fault schedule (Ref. 131) to the 'BSC of Protection System' (Ref. 99) because the names of requirements were different between these two documents. I raised RQ-UKHPR1000-1419 (Ref. 109) requesting clarification on specific functions identified, but also more generally how it is shown the system requirements are complete and unambiguous. My assessment of the response to this RQ identified that it is not possible to confirm the correct linkage between the fault schedule, the BSC and the SRS, or to confirm that there are no requirements in the SRS that do not trace back to the BSC and fault schedule.

279. My assessment identified several shortfalls in the way that requirements are specified and managed. These can be summarised as follows:

- Sources of requirements could not be identified, including requirements from the safety analysis, higher level principles, those from non-C&I technologies (e.g. mechanical, electrical, human factors, etc.), operations, test, maintenance, repair, etc.

- It was not clear that all functional and non-functional requirements were defined.
- Unwanted behaviours were not identified, and no requirements were specified to ensure that these are actively avoided.
- Requirements were often not atomic (i.e. containing only one concept or actionable element).
- Requirements could not be unambiguously traced both forwards and backwards through the design process and documentation.
- Requirements were ambiguously documented, and terminology was often inconsistent.
- It was often not possible to identify a single point of origin for individual requirements.
- C&I requirements originating from other technical areas could not be identified, and it was not clear how these are effectively and unambiguously exchanged with these other technical areas.
- Limitations, assumptions, constraints and conflicts were not clearly and unambiguously documented.
- It was not clear how the potential for errors (including human and technological) in the manipulation, translation and use of requirements will be effectively managed.
- Requirements were not complete, unambiguous, and consistent through documentation, and across the wider project.

280. These are significant shortfalls, and without these issues being addressed it is not possible to demonstrate that the RPS [PS] will perform the functions specified, and that it will not perform other functions not specified, potentially leading to a safety consequence. I observe that the same shortfalls exist for the requirements relating to other C&I systems (see sub-sections 4.6.2 – 427). I consider these shortfalls to be of sufficient importance that they should be tracked to resolution and have therefore raised an Assessment Finding.

AF-UKHPR1000-0034 – The licensee shall establish a mechanism by which the requirements for UK HPR1000 C&I platforms and systems can be unambiguously and completely established and managed, and that this can be demonstrated to be so, ensuring that:

- all functional and non-functional requirements are defined;
- the source of each individual requirement is identified;
- requirements contain only one concept or actionable element;
- requirements can be unambiguously traced both forwards and backwards through the design and safety case documentation;
- requirements are complete, unambiguous and consistently documented;
- assumptions and constraints are clearly and unambiguously documented; and
- the potential for errors in the manipulation, translation and use of requirements is minimised.

281. The ONR cross-cutting assessment report (Ref. 201) has also identified significant shortfalls with the management of requirements across the project and has raised Assessment Findings AF-UKHPR1000-0107 – AF-UKHPR1000-0110 for these shortfalls to be addressed. My expectation is that the resolution of Assessment Finding AF-UKHPR1000-0034 will consider these broader cross-cutting findings.

Application of Standards and Demonstration of Production Excellence

282. I also wanted to confirm that appropriate standards have been applied to the development of the RPS [PS], as described in SAPs ECS.3, ESS.27 and ESR.5. My assessment was informed by relevant RP submissions, including:

- ‘Demonstration of Production Excellence for the RPS [PS]’ (Revision C) (Ref. 202).
- ‘Application Software Verification and Validation Plan of FirmSys Based I&C Systems’, (Revision A) (Ref. 203).
- ‘Comparison of Protection System RPS [PS] with IEC 61513’ (Ref. 204)
- ‘Comparison Analysis of Protection System (RPS [PS]) with IEC60880’ (Ref. 205)
- ‘Comparison Analysis of FirmSys Based I&C Systems with IEC 60987’ (Ref. 206)

283. My assessment identified that appropriate high-level standards have been specified (e.g. IEC 61513 (Ref. 21), IEC 60880 (Ref. 16), IEC 62566 (Ref. 24), IEC 60987 (Ref. 17), etc.), for the RPS [PS]. However, I identified shortfalls in the evidence provided for claims of compliance with specific standards clauses, such as in the areas of the suitability and use of software-based tools, hardware requirements, nature and depth of reviews, and recording of verification and validation results.

284. To further understand the suitability of the system development processes, I requested that detailed samples of evidence relating to three functions be provided, RPS-SRS-022 “Overpower ΔT”, RPS-SRS-0045 “RIS [SIS]/RHR pump trip on ΔPsat low 2”, and RPS-SRS-0285 “Self supervision”; these were submitted in three documents (Ref. 207), (Ref. 208), (Ref. 209). These provided information on the system development processes, but did not provide the evidence I was seeking regarding the application of appropriate standards.

285. In respect of compliance with IEC 61513 my assessment revealed a number of significant shortfalls in the areas of clarity of requirements and traceability, review criteria, test coverage, and hardware requirements that, taken together, mean that it is not possible to determine that the safety functions have been completely and unambiguously specified, correctly implemented, or demonstrated to be so.

286. In respect of compliance with IEC 60880, I identified additional shortfalls including lack of system requirements (e.g. security), inappropriate expectation that system requirements would be identified and met by application engineering personnel, incorrect application of the intent of standards clauses, and lack of clarity of V&V personnel roles and responsibilities. My additional assessment of the Application Software Verification and Validation Plan of FirmSys Based I&C Systems (Ref. 203) identified further shortfalls, including ambiguity regarding the configuration management arrangements between the system and platform.

287. I raised a number of queries relating to the RPS [PS] submissions in the following RQ’s (Ref. 109):

- RQ-UKHPR1000-0973, relating to the lifecycle approach to design, the suitability of the quality management system, the application of RGP, and future plans.
- RQ-UKHPR1000-1010, relating to omission of important codes and standards including IEC 61226, IEC 62340.
- RQ-UKHPR1000-1270, relating to the application software V&V plan.
- RQ-UKHPR1000-1354, relating to a comparison between the requirements of IEC 60880, and the RPS [PS] development approach.
- RQ-UKHPR1000-1591, relating to the RPS-SRS-022 “Overpower ΔT” PE sample.
- RQ-UKHPR1000-1743, relating to inputs into the PE of RPS [PS], Rev. C.
- RQ-UKHPR1000-1750, relating to the RPS-SRS-0285 “Self supervision” PE sample.

288. I assessed the responses to these RQ's and identified that whilst some queries had been satisfactorily answered, a significant number of queries had either not been addressed, or only partially addressed.

289. In response to this finding, the RP undertook a self-assessment of the RPS [PS] PE evidence. This considered the applicability of the gaps that had been identified in the FirmSys PE evidence to the RPS [PS]. This was submitted as 'Demonstration of Production Excellence for the RPS [PS]' (Ref. 202). This identified gaps in the RPS [PS] PE evidence, including in the areas of requirements management, overall development approach, and hardware and software development, and in accordance with the expectations of SAP ESS.27 proposed compensating measures to resolve these.

290. Whilst the RP has identified compensating measures for each gap, the number of gaps, their wide-ranging nature and their significance, is an area of concern. I cannot confirm the suitability of the CMs to address the PE gaps identified during GDA, as these will involve changes being made to processes, competence arrangements, and design approaches. I judge that the shortfalls identified have the same causes as those identified in the FirmSys platform section of this report, and for which raised AF-UKHPR1000-0031 has been raised (see sub-section 195). Furthermore I have raised AF-UKHPR1000-0024 (see Section 4.3), to ensure that a comprehensive review is undertaken of the UK HPR1000 C&I systems against the requirements of international standards. However, I consider it important that a complete and comprehensive demonstration of PE is produced for the RPS [PS]. Given the gaps highlighted by the RP in (Ref. 202) it cannot currently be concluded that there is adequate PE for the RPS [PS], and hence I have raised an Assessment Finding for this to be addressed by the licensee.

AF-UKHPR1000-0035 – The licensee shall demonstrate the production excellence of the detailed design UK HPR1000 computer-based C&I systems important to safety, using an equivalent methodology to that applied to the Class 1 FirmSys platform during GDA. This shall give particular consideration to the following, as a minimum:

- the identified safety objectives of the platform and systems;
- the need to implement measures to control the effects on system operation of internal failures and faults; and
- all reactor operating modes for which the systems are required to act.

Safety Properties

291. I assessed the adequacy of the RPS [PS] documentation in respect of important safety properties, considering the following SAPs:

- EDR.1 Failure to safety;
- EDR.2 Redundancy, diversity and segregation;
- EDR.3 Common Cause failure;
- ESS.1 Provision of safety systems;
- ESS.5 Plant interfaces;
- ESS.8 Automatic initiation;
- ESS.17 Faults originating from safety systems;
- ESS.18 Failure independence;
- ESS.21 Reliability; and
- ESS.27 Computer-based safety systems.

292. The RP submissions that I assessed in this area included:

- ‘BSC of Protection System’ at Revisions C (Ref. 210), E (Ref. 163) and F (Ref. 99);
- ‘UK HPR1000 Fault Schedule’ (Ref. 131);
- ‘RPS [PS] System Requirements Specification’ (Ref. 151);
- ‘FMEA Report of Protection System’ (Ref. 114);
- ‘Demonstration of Production Excellence for the RPS [PS’] (Ref. 202);
- ‘Strategy for Conducting ICBMs Activities for RPS [PS’] at Revision C (Ref. 211); and
- ‘Design Specification of Protection System RPS [PS]’ at Revision E (Ref. 212).

293. For each of the SAPs I was able to identify relevant claims in Revision C of the RPS [PS] BSC (Ref. 210), and requirements associated with these.

294. As an example, for EDR.1 I was able to identify requirements relating to this in the RPS [PS] SRS (Ref. 151), including the requirement that failures shall be detectable [SRS-0183], and loss of power will cause the RPS [PS] to enter a pre-determined condition acceptable for safety [SRS-0181]. However, I was unable to follow these requirements through to specific design features or to understand how the intent of the requirement has been met.

295. I raised a number of RQs (Ref. 109) to try to improve my understanding, including:

- RQ-UKHPR1000-1057 Regulatory Query - Protection System - Faults Originating from Safety System.
- RQ-UKHPR1000-1061 - Regulatory Query - Protection System – Safe State.
- RQ-UKHPR1000-1062 Regulatory Query - Protection System - Provision of Controls and Automatic Initiation/
- RQ-UKHPR1000-1167 - Failure Mode and Effects Analysis.

296. My assessment of the responses to the RQs (Ref. 109) identified similar shortfalls to those raised earlier in this report, namely a lack of traceability of requirements, and limitations in failure analyses. This is already addressed by Assessment Findings AF-UKHPR1000-0034.

297. I considered the extent to which the development of the RPS [PS] makes appropriate use of technology and based my assessment on ESS.19, ERL.1 and ERL. 2.

298. I was satisfied that the RPS [PS] is dedicated to a single task, and that potential interference between different safety functions is inherently managed through the design approach of both the RPS [PS] and the FirmSys platform on which it is based. I was also satisfied that the form of the claims was suitable at a high-level. It was not possible to completely trace all the resultant requirements through to system design features.

299. Revision C of the RPS [PS] BSC (Ref. 210) identified the high-level functional claims on the RPS [PS], and these are decomposed into sub claims, supported by arguments and evidence. I was generally satisfied by the CAE form of the safety case, but raised RQ-UKHPR1000-1238 (Ref. 109), specifically relating to the argument that “the RPS [PS] is developed to the Safety Integrity Level (SIL) 4 Level of IEC 61508” without adequate justification. This argument was removed, and the BSC of the Protection System re-submitted (Ref. 163). Whilst further safety case is necessary during the detailed design and substantiation of the RPS [PS], I judge that the safety case for the RPS [PS] is sufficiently developed for the purposes of GDA.

300. My assessment of Revision E of the RPS [PS] BSC (Ref. 99) in respect of ERL.2 identified that it is difficult to determine that all appropriate measures to demonstrate adequate reliability have been considered, that the measures identified are coherent, that all the measures together will result in adequate reliability, and what, if any,

constraints this may place on the design of the system. For example, periodic testing is identified, but it is not clear how this will place requirements on the system, how these will affect system design, how frequent this should be for the claimed reliability to be achieved, and any limitations this may place on system design. This is a potential shortfall, as this will be necessary to demonstrate that the system design is suitable, considering practical constraints, such as testing whilst the reactor is at power. This point is covered by Assessment Finding AF-UKHPR1000-0030 (see Section 175).

301. I assessed the ability of the RPS [PS] to function in the environmental conditions it could experience, focusing on temperature. I did this by first determining the environment in which the C&I cabinets would be installed, and then by assessing whether the qualification approach and evidence for the RPS [PS] supports this. The submission 'Analysis Report of the HVAC Sample Systems' (Ref. 213) estimates what conditions will be present in a variety of equipment rooms under various plant conditions. This analysis identified that a maximum temperature of nearly 43°C could occur in some C&I equipment rooms under certain HVAC failure conditions. Recognising that the RPS [PS] is implemented using FirmSys components, I assessed the submission 'Equipment Qualification plan of FirmSys Platform' (Ref. 214) to understand how it is demonstrated that the RPS [PS] will continue to function under these conditions. I found that environmental tests are performed on a representative system consisting of FirmSys components in a fully populated cabinet, that the system is energised, that the performance of the system is monitored throughout the tests, and that tests are performed for 300 hours at both 40°C and 55°C external cabinet temperatures. The submission 'Report on Equipment Qualification Test for FirmSys Platform Main-Control' (Ref. 215) provides a record of tests that have been performed, and records that the tests were passed. I note that further detail on equipment qualification will be required to underpin the safety case; I expect that this will be addressed by the licensee as part of normal business during the detailed design and substantiation of the RPS [PS]. Based on the evidence sampled I was satisfied that this evidence was suitable for the purposes of GDA.

Influence from Lower-class Systems

302. I considered the potential for the RPS [PS] to be influenced by lower-class systems, considering the following submissions:

- 'RPS [PS] System Requirements Specification' (Revision D) (Ref. 151).
- 'BSC of Protection System' (Revision F) (Ref. 99).
- 'Design Specification of Protection System RPS [PS'] (Revision D) (Ref. 212).
- 'Independence Analysis of I&C Systems' (Revision D) (Ref. 142).

303. My assessment of the BSC of the protection system identified claims that the RPS [PS] is not influenced by lower-class systems. I determined from the 'RPS [PS] System Requirements Specification' (Ref. 151) that the RPS [PS] does not rely on signals from lower-class systems for operation. The classification of systems generating permissive signals is covered in Section 500 on HMI, and the remainder of the systems that are connected to the RPS [PS] are covered Section, 4.3 of this report, and so are not covered further in this section.

Examination, Maintenance, Inspection and Testing

304. My assessment of EMIT at the architectural level is documented in Section 175. I also considered whether the approach to testing and maintenance of the RPS [PS] meets UK regulatory expectations. For this topic I considered the following SAPs:

- EAD.1 Safe working life;
- EAD.2 Lifetime margins;
- EMT.7 Functional testing;

- ESS.23 Allowance for unavailability of equipment;
- ESS.25 Taking safety systems out of service; and
- ESS.26 Maintenance and testing.

305. The submissions that I assessed in this area included:

- 'RPS [PS] - Reactor Protection System Design Manual Chapter 6 System Operation and Maintenance' (Ref. 216).
- 'BSC of Protection System' (Ref. 99) .
- 'Periodic Test Requirement of Protection System (PS)' (Ref. 217).
- 'Design Specification of Protection System RPS [PS]' (Ref. 218).

306. My assessment identified that the 'Reactor Protection System Design Manual Chapter 6 System Operation and Maintenance' (Ref. 216) (SDM) is not referenced in the BSC of the Protection System, so it is was not clear how the information in this document fitted into the overall safety case. I raised RQ-UKHPR1000-1055 (Ref. 109) to query this. The response to RQ-UKHPR1000-1055 (Ref. 109) indicated that the SDM is outside the scope of GDA, so I did not consider this document further.

307. I noted that the 'BSC of Protection System' (Ref. 99) contains claims regarding operational life, but these are not substantiated, other than referring to equipment qualification with no further detail on how this relates to operational life. Similarly, there are claims regarding equipment qualification and its suitability during normal and accident conditions, but there is no reference to accident studies, hazard analyses, or risk assessments to underpin this claim. This has been taken forward under AF-UKHPR1000-0052 (see sub-section 4.11) and is not discussed further in this section.

308. Some information is presented in relation to functional testing, allowance for the unavailability of equipment, taking systems out of service, and maintenance and testing. For example, in respect of taking systems out of service the change in the voting arrangements is described. However, it is not clear if this is a system requirement based on a higher level requirement, or just a description of how the system is designed.

309. In respect of maintenance and testing, the use of overlapping sequential tests is described in 'Periodic Test Requirement of Protection System' (PS) (Ref. 217), but this high-level objective is not supported by evidence that shows how all faults can be detected, and whether there are any RPS [PS] faults that are not detected. I raised RQ-UKHPR1000-1751 (Ref. 109) to query this for the SAS periodic test (as both systems are based on the FirmSys platform); this is reported in sub-section 4.6.2 of this report, so is not reported further here, other than to note that the same shortfalls appear to exist for both systems.

310. I am of the opinion that the shortfalls I have identified in respect of testing and maintenance arise from deficiencies in requirement traceability, which in turn has resulted in there being a lack of referenced evidence to support the claims and arguments made. These shortfalls have been captured in AF-UKHPR1000- AF-UKHPR1000-0034 (see sub-section 4.6.1).

311. I considered whether the arrangements for RPS [PS] system function and parameter configuration control are adequate, using SAP ESS.15 and IEC 61513 to guide my assessment. I assessed 'Comparison of UK HPR1000 Protection System RPS [PS] with IEC 61513' (Ref. 88), and noted that a maintenance tool is used to perform monitoring, diagnosis, maintenance, etc. Also that the maintenance tool may only alter application software or configuration parameters when the RPS [PS] channel is out of service, and that it is physically disconnected when not in use. I raised RQ-UKHPR1000-1220 (Ref. 109) to request further information regarding the physical, maintenance QA and configuration management arrangements. The response only

partially answered the queries. In particular, whilst some information was given regarding how connection of the maintenance tool to more than one division is prevented, it was not stated what detailed arrangements are in place to control the connection or use of the maintenance tool. Similarly, the integrity of the maintenance tool was not described, nor how it is confirmed that the correct application software and parameter configuration is set.

312. I consider it important that the correct application software and parameter configuration is set, as if these are incorrect, the RPS [PS] will not perform the safety functions as expected. I judge this to be sufficiently important that I have raised an Assessment Finding:

> AF-UKHPR1000-0036 – The licensee shall demonstrate that the risks arising from misconfiguration of the Reactor Protection System and Safety Automation System through use of the software maintenance tool are reduced so far as is reasonably practicable, by:
>
> - identifying the hazards arising from the connection and operation of the Reactor Protection System and Safety Automation System maintenance tool, including from inadvertent connection, incorrect use, software or hardware faults, cyber threats.;
> - identifying measures to control these hazards, considering a hierarchy of controls, with engineered controls being more reliable and administrative controls being less reliable; and
> - demonstrating that the controls will be effective to control the identified hazards, and suitably reliable.

Avoidance of Spurious Actuation

313. My assessment of the RP's analysis of the consequences of spurious actuation is documented in sub-section 4.3.1.4. I also considered the suitability of the RPS [PS] in respect of the avoidance of spurious actuation, using SAP ESS.22 and IEC 61513 to guide my assessment.

314. The submissions that I assessed in this area included:

- 'BSC of Protection System (Revision F)' (Ref. 99).
- 'RPS [PS] System Requirements Specification' (Revision D) (Ref. 151).
- 'Design Specification of Protection System RPS [PS]' (Revision D) (Ref. 212).

315. My assessment identified that the 'BSC of Protection System' (Ref. 99) includes a number of claims relating to avoidance of spurious actuation, including functional separation and functional independence, arrangements for majority voting, and bypasses to allow maintenance activities to be carried out without inadvertent activation of a safety function.

316. The submission 'Design Specification of Protection System RPS [PS]' (Ref. 212) provides further information on arrangements to manage the risk of spurious actuation, including self-supervision to detect faults, the use of confirmatory signals to avoid of spurious actuation from manual controls, and equipment qualification to manage spurious actuation arising from environmental, seismic, and electromagnetic effects.

317. Whilst I consider these all to be relevant to risks arising from spurious actuation, it is my opinion that this does not provide a complete safety case demonstrating that all potential causes of spurious actuation have been identified and measures to prevent these put in place. For example, there is no evidence that self-supervision is adequate

in all cases to detect faults and prevent spurious actuation. Similarly, it is possible that spurious actuation could be caused by a software fault that is present in all divisions.

318. I judge that the above points are exacerbated by a lack of clear requirements for the RPS [PS] in relation to spurious actuation arising from within the system, and that this is repeated for each of the other centralised C&I systems. I consider this is sufficiently important for progress with the safety case for each of the centralised C&I systems to be tracked to completion during site-specific stages of the project. For this reason, I have raised the following Assessment Finding:

AF-UKHPR1000-0037 – The licensee shall demonstrate that the frequency of spurious actuation of the UK HPR1000 C&I systems important to safety is minimised as low as reasonably practicable, considering: ■ the architectural arrangement; ■ the potential for faults to occur due to hardware failures; ■ the potential for errors to occur in digital communications; and ■ the potential for common cause software failures to occur.

4.6.1.2 Strengths

319. During GDA Step 4 the RP has improved the RPS [PS] safety case structure and content. This has resulted in greater clarity of intent and better linked the evidence to the claims and arguments.

320. The RP has developed a CAE structure that is sufficiently well developed for GDA, and this includes claims to address key safety properties.

4.6.1.3 Outcomes

321. My assessment identified shortfalls in the areas of requirements specifications which are exacerbated by the last of clear requirements for the RPS [PS]. I am of the opinion that this shortfall is common for all UK HPR1000 systems and I have raised AF-UKHPR1000-0037 to ensure that this is adequately addressed by the licensee.

322. I observed that suitable standards have been referenced in relation to the RPS [PS]. I found that the RPS [PS] safety case structure met my expectations for GDA, but the evidence did not always support the arguments and evidence; this issue is also common across systems and is addressed by AF-UKHPR1000-0052 (see Section 4.11).

323. During GDA step 4 the RP identified shortfalls in the RPS [PS] PE and have raised AF-UKHPR1000-0035 to ensure this is resolved during site-specific stages of the project.

324. I identified a concern regarding the completeness of evidence regarding potential for misconfiguration of the RPS [PS] and have raised AF-UKHPR1000-0036.

325. I also identified a concern regarding the evidence to document measures to prevent spurious actuation of the RPS [PS], and have raised AF-UKHPR1000-0037.

4.6.1.4 Conclusion

326. In conclusion, I judge that sufficient information has been provided for a meaningful assessment of the RPS [PS] system to be carried out that is sufficient for the purposes of GDA. Appropriate standards have been identified and standards compliance analysis has been performed. However, I have found that sufficient evidence has not been provided to demonstrate how all relevant standards clauses have been met. Similarly, I found that the safety case is not always adequately supported by evidence. As with the other UK HPR1000 systems I found that the system requirements have not

been clearly and completely established, and I could not confirm that the intent of the system functions and properties has been met by the system design, and that relevant SAPs, such as EDR1, ESS.18, and ERL.2, have been satisfied. These issues have been taken forward as Assessment Findings.

4.6.2 Adequacy of the SAS

4.6.2.1 Assessment

327. The 'BSC of Safety Automation System' (Ref. 100) contains claims that the SAS system performs a range of FC2 (Category B) safety functions such as manual and automatic functions to bring the reactor from a controlled state to a safe state following DBC-2, DBC-3 and DBC-4. It also performs the Design Extension Condition (DEC)-A feature functions and other FC2 control and monitoring functions (e.g. the control of supporting systems). I assessed the SAS on the basis that this is a Class F-SC2 (Class 2) system performing FC2 (category B) safety functions. The SAS is implemented using the FirmSys platform.

System Requirements

328. I wanted to confirm that adequate system requirements have been identified for the SAS. My assessment considered a range of SAPs including ESS.10 and ESS.11 relating to capability and adequacy, as well as IEC 61513 (Ref. 21), and was informed by relevant RP submissions, including:

- 'UK HPR1000 Fault Schedule' (Ref. 131).
- 'BSC of Safety Automation System' (Revision C) (Ref. 100).
- 'SAS System Requirements Specification' (Revision D) (Ref. 106).
- 'Design Specification of Safety Automation System (SAS)' (Revision D) (Ref. 219).
- 'UK HPR1000 Confinement Schedule' (Ref. 220).

329. The SAS BSC (Ref. 100) describes a number of safety functions using a CAE structure. This structure is suitable to form the basis for argumentation for the SAS.

330. I assessed the adequacy of the tracing of requirements between the BSC (Ref. 100), the 'SAS System Requirements Specification' (Ref. 106), and the 'Design Specification of Safety Automation System' (SAS) (Ref. 219) and found that the logic type functions could be traced from the BSC to the SRS, and that they are repeated in the SDS. I noted that some functions do not appear to be linked to the fault schedule (Ref. 131), but that the complementary confinement functions sampled are included in the confinement schedule (Ref. 220).

331. I observed that functions do not appear to be further elaborated in the different documents and it is not clear what the repetition is intended to achieve. I consider this shortfall to be similar to that identified for the RPS [PS], and for which RQ-UKHPR1000-1419 (Ref. 109) was raised. This is addressed in the RPS [PS] section of this report (see sub-section 4.6.1); I consider that AF-UKHPR1000-0034 is suitable to address the shortfalls identified for the SAS.

332. I also wanted to confirm that appropriate standards have been identified for the development of the SAS, as expected by SAPs ECS.3, EQU.1, and ESR.5. My assessment was informed by relevant RP submissions, including:

- 'Comparison Analysis of Safety Automation System (SAS) with IEC 62138' (Ref. 91).
- 'BSC of Safety Automation System' (Ref. 100).
- 'Demonstration of Production Excellence for the SAS' (Ref. 221).

333. My assessment identified that appropriate high-level standards have been specified for the SAS (e.g. IEC 61513 (Ref. 21), IEC 62138 (Ref. 22), IEC 60987 (Ref. 17), etc.).

334. However, I identified shortfalls in the evidence provided for specific standards clauses, for example in the areas of the software modification and defences against CCF of software in IEC 62138 because the RP does not consider these to be in scope. Whilst these activities may not be applied until later in the software development, it is my expectation that they will be appropriately planned, and processes developed to ensure they meet the requirements of the relevant standards.

335. I also noted inconsistency in respect of the evidence provided to support specific standards clauses, in that the evidence for some standards clauses precisely references and argues the suitability of that evidence, whilst other clauses do not. In addition, it appears that the intent of some standards clauses has not been understood, such as IEC 62138 clauses 6.5.3.6 software implementation rules for Class 2, and 6.8.6 traceability between the software requirements and validation actions for Class 2. I raised RQ-UKHPR1000-1355 (Ref. 109), to further understand the causes of these shortfalls. The response acknowledged a number of shortfalls and indicated that these would be resolved during site-specific stages of the project. My expectation is that these minor shortfalls will be addressed as part of normal business as the detailed design of the SAS progresses.

336. I assessed Revision C of 'Demonstration of Production Excellence for the SAS' (Ref. 221), in which the RP identified similar shortfalls to those in the equivalent document for the RPS [PS], with a total of sixteen shortfalls identified in the areas of requirements management, security analyses, lack of detail in verification records, lack of process records for design review, etc. I noted that there were two areas where gaps that were identified for the RPS [PS] have not been identified in the SAS PE demonstration; these relate to Configuration Management and Test Configuration Environment. I judge this discrepancy between the analyses of the RPS [PS] and the SAS to be a shortfall which reduces my confidence in the suitability of the analysis.

337. I consider it will be necessary for the PE analyses to be repeated for the detailed design of the SAS, considering the limitations identified in these documents, and in the comparison of the SAS with the IEC 62138 document (Ref. 91). This is covered by Assessment Findings by AF-UKHPR1000-0024 (see Section 41) and AF-UKHPR1000-0035 (see sub-section 4.6.1).

338. I assessed the suitability of the SAS ICBMs under the section on ICBMs (Section 4.7).

Safety Properties

339. I assessed the adequacy of the SAS documentation in respect of important safety properties, primarily considering the following SAPs:

- ESS.21 Reliability; and
- ESS.27 Computer-based safety systems.

340. The RP submissions that I assessed in this area included:

- 'BSC of Safety Automation System' (Ref. 100).
- 'Centralised I&C System Reliability Study Report' (Ref. 57).

341. My assessment of the suitability of the SAS against ESS.21 (reliability), found that the SAS BSC includes arguments that the reliability of the SAS is demonstrated by variety of methods, including a hardware reliability model, FMEAs, testing, and system modelling. However, the evidence cited to support these arguments is either

requirements specifications, or test plans, procedures, and reports, except for the document 'Centralised I&C System Reliability Study Report' (Ref. 57).

342. I assessed the 'Centralised I&C System Reliability Study Report' (Ref. 57) and concluded that there was insufficient evidence to support the arguments made in the BSC for which this document is cited as evidence. However, I noted that it is stated that component level FMEA will be undertaken on the SAS during site-specific stages of the project. I also noted that the document provides an overview of the methodology that will be used to assess the reliability of the SAS design, covering hardware reliability, the effects of failures considering the architectural arrangement, and the causes and effects of software faults. On the basis of the evidence assessed I judge the methodology to be appropriate. However, it is my expectation that further work should be undertaken to demonstrate the suitability of the methodology and to justify the system reliability. This is addressed by Assessment Finding AF-UKHPR1000-0026 (see Section 4.3).

343. I considered the extent to which the development of the SAS makes appropriate use of technology, and considered ESS.19, dedication to a single task, ERL.1 form of claims, and ERL. 2 measures to achieve reliability.

344. My assessment found that the 'BSC of Safety Automation System' (Ref. 222) identifies the high-level functional claims on the SAS, and that these are appropriately decomposed into sub claims. I was satisfied that the SAS tasks were clearly defined, and that potential interference between different safety functions is inherently managed through the design approach. I was also satisfied that the form of the claims was suitable at a high-level and that the 'SAS System Requirements Specification' (Ref. 106) identified SAS requirements.

345. In respect of reliability, I note that the SAS is implemented on the FirmSys platform which is claimed to have mechanisms to detect and manage failures such as hardware failures and is also claimed to be able to achieve a higher reliability than is required for the SAS. I also note that the SAS uses a three division architecture and redundancy that is tolerant to failures. I am satisfied that, subject to a suitable and sufficient safety case being developed during the site-specific stages, and the correct application of appropriate safety features, that the SAS is likely to be capable of achieving the reliability claimed.

Influence from Lower-class Systems

346. I considered the potential for the SAS to be influenced by lower-class systems, considering the following submissions:

- 'BSC of Safety Automation System' (Revision C) (Ref. 100).
- 'SAS System Requirements Specification' (Revision D) (Ref. 106).
- 'Design Specification of Safety Automation System (SAS)' (Revision D) (Ref. 219).

347. The 'BSC of Safety Automation System' (Ref. 222) contains claim C2.1.3.1.4 "The SAS is adequately separated from lower tiered systems to limit the possibility of fault propagation.", and presents a number of arguments, including a description of hardwired and digital communication links to lower-class systems. However, whilst some links are described as unidirectional, others are not, leading to a concern that some links may be bidirectional. The evidence for this refers to Section 8.2 of the SAS SRS (Ref. 106) and Appendix C of the SDS (Ref. 219).

348. I assessed Section 8.2 of the SAS SRS and found that this lists each interface between the SAS and other systems, and that where a digital communication link is used, these are described as unidirectional from the SAS, except in the case of the

communication between the RPS [PS] and the SAS, where the communication is one-way from the RPS [PS] to the SAS. This is acceptable as there is no communication link from lower to higher-class systems.

349. My assessment of Appendix C of the 'Design Specification of Safety Automation System (SAS)' (Ref. 219) identified the same information presented in a different form. However, I noted that there appears to be a hardwired signal between the lower-class PSAS to the SAS, with limited description "Some interlock signal are sent from PSAS to SAS" and no argument as to why this is acceptable. It is a concern that this signal is described as an interlock signal, and there is insufficient information presented as to the consequences on the behaviour of the SAS of this signal being in the wrong state. I was unable to determine whether there are other signals that could affect the behaviour of the SAS; I judge this to be a minor shortfall which should be addressed as part of normal business during detailed design of the system.

350. I am generally content that sufficient evidence has been presented during GDA that there are adequate measures in place to prevent the influence of lower-class systems on the SAS by digital communication means.

351. However, there is evidence of at least one hardwired link that could affect the correct operation of the SAS. During the detailed design of the SAS, a thorough analysis of the behaviour of all input and output signals should be undertaken; I expect that this will be done as part of normal business. I am concerned, however, that hardwired links from lower class systems has the potential to affect the correct operation of the SAS and I judge this to be a shortfall that should be tracked to resolution. I have therefore raised an Assessment Finding for this to be addressed during detailed design.

AF-UKHPR1000-0038 – The licensee shall demonstrate that hardwired inputs to the Safety Automation System from lower safety classified systems cannot compromise delivery of the Safety Automation System safety functions.

Testing and Maintenance

352. I considered whether the approach to testing and maintenance meets UK regulatory expectations. For this topic I considered the following SAPs:

- EAD.1 Safe working life;
- EAD.2 Lifetime margins;
- EMT.7 Functional testing;
- ESS.23 Allowance for unavailability of equipment;
- ESS.25 Taking safety systems out of service;
- ESS.26 Maintenance and testing.

353. The submissions that I assessed in this area included:

- 'BSC of the SAS' (Revision C) (Ref. 100).
- 'SAS System Requirements Specification' (Revision D) (Ref. 106).
- 'Design Specification of Safety Automation System (SAS)' (Revision D) (Ref. 219).

354. In respect of EAD.1 I found that the 'BSC of the SAS' (Ref. 100) contains claim C2.2.2 relating to "operational life", and that arguments associated with this claim relate to qualification and adherence to standards. It is not clear what the requirements for operational life are, and how this is linked to qualification or adherence to standards. However, I note that claim C5.2.2 states that "The components within the SAS having service life limits due to age related failure mechanisms are regularly replaced to keep reliability.", and that arguments supporting this claim include:

- "A2 Measures are taken in the SAS design to facilitate equipment replacement"; and
- "A3 Maintenance will be managed in accordance with a comprehensive operation and maintenance manual."

355. The evidence offered for the facilitation of equipment replacement includes sufficient space reserved for further system expansion or modification.

356. I also noted that argument A3 under claim C2.1.3.2 "The SAS is designed to be fail safe" includes a reference to the management of ageing and obsolescence. Whilst little detail has been provided during GDA regarding safe working life, I consider this to be sufficient for GDA.

357. In respect of EAD.2 I noted that claim C5.2.2 is relevant to this, and whilst there is little detail available during GDA, I was content that there was consideration of lifetime margins, noting that detail will need to be added to the safety case in this area post GDA.

358. In respect of EMT.7 I noted that there are a number of claims in the BSC of the SAS relating to this, including:

- "C5.2.1.1 The SAS is designed to allow a periodical and sufficiently complete testing to detect failures which are not self-announced."
  - "A2: The periodic testing of the cabinets is performed by sequential and overlapped tests."
  - "A3: The allowable EMIT window of the cabinets is determined."
- "C5.2.1.2 The SAS includes the platform self-diagnosis and application self-diagnosis for the identification of faults."
  - "A1: The platform self-diagnosis is integrated in the system software and run at a fixed cycle."
  - "A2: The application self-diagnosis is supplement to the platform self-diagnosis and realised by the engineering application."

359. The evidence relating to sequential and overlapping tests is provided in Section 13 of the 'SAS System Requirements Specification' (Ref. 106), where a number of requirements are identified, including "Simultaneous testing from sensor to actuated equipment is preferred. Where it is not practical, the overlap testing capability shall be provided. [SAS-SRS-0255]". I also note that it is stated "The extent of periodic testing shall include all aspects of the sensor, the input signal, the final actuator and the display. [SAS-SRS-0254]". Whilst sequential and overlapping tests may be able to achieve this requirement, it was not clear from the information provided how this would be achieved, so I raised RQ-UKHPR1000-1751 (Ref. 109), to request further information in the areas of test coverage, the extent to which self-supervision tests are relied on, which failures are covered by the tests, and which are not. The response provided further details and stated that test coverage is considered complete with the exception of a small number of automatic control application functions, self-supervision tests are relied on internally within the SAS, and that diagnosable failures are covered, noting that further work will be done at site-specific stages to identify failures.

360. I note that the approach to periodic testing is similar to that for the other central C&I systems. Whilst this is an acceptable response for GDA, I consider the importance of this topic to be such that it should be tracked through to completion. My expectation is that this will be addressed as part of AF-UKHPR1000-0030 (see Section 175).

361. I considered whether SAP ESS.15 “Alteration of configuration, operational logic or associated data” and the relevant parts of IEC 61513 have been satisfied by the SAS system design and documentation.

The submissions that I assessed in this area included:

- ‘BSC of Safety Automation System’ (Revision C) (Ref. 100).
- ‘SAS System Requirements Specification’ (Revision D) (Ref. 106).
- ‘Design Specification of Safety Automation System’ (SAS) (Revision D) (Ref. 219).

362. I identified that Claim C5.2.1.3 in the ‘BSC of Safety Automation System’ (Ref. 100) states “Alteration of the SAS configuration, operational logic or associated data is only able to be performed under strict administrative controls.”. The evidence supporting this is in Section 13.4.3 of the SAS SRS (Ref. 106). However, I found there to be a lack of detail in this document or the supporting SDS (Ref. 219), particularly in the area of engineered controls to prevent misconfiguration. Whilst administrative controls are important, engineered controls are also important in preventing incorrect changes to the SAS application or its parameters. This shortfall is the same as that identified for the RPS [PS], as both the RPS [PS] and the SAS share a common platform in FirmSys, and is therefore addressed through AF-UKHPR1000-0036 (see sub-section 4.6.1).

Avoidance of Spurious Actuation

363. I considered the suitability of the SAS in respect of spurious actuation, using SAP ESS.22 and IEC 61513 to guide my assessment.

The submissions that I assessed in this area included:

- ‘BSC of Safety Automation System’ (Revision C) (Ref. 100).
- ‘SAS System Requirements Specification’ (Revision D) (Ref. 106).
- ‘Design Specification of Safety Automation System (SAS)’ (Revision D) (Ref. 219).

364. My assessment identified that the SAS BSC (Ref. 100) includes a claim relating to avoidance of spurious actuation, “C2.1.3.6 The design of the SAS considers the means to avoid the spurious actuation.”. This is supported by argument A1 “The spurious actuation caused by common cause failure of SAS is analysed.”. However, none of the argumentation refers specifically to the SAS, and in particular the system features and architecture. I was therefore not able to determine that the causes of spurious actuation arising from the SAS have been identified and adequately managed. However, I note that these shortfalls are similar to those identified for the RPS [PS], and for which Assessment Finding AF-UKHPR1000-0037 (see sub-section 4.6.1) has been raised. This finding covers all UKHPR1000 C&I systems important to safety, and as a result I consider that no further action is necessary for the SAS.

4.6.2.2 Strengths

365. During GDA Step 4 the RP has improved the SAS safety case structure and content. This has resulted in greater clarity of intent and better linked the evidence to the claims and arguments.

366. I observed that suitable standards have been referenced in relation to the SAS.

4.6.2.3 Outcomes

367. My assessment found that the design of the SAS has adequately considered the potential for safety functions to interfere with each other, and has implemented

measures to prevent digital communications from lower-class systems impacting on the SAS safety functions.

368. My assessment identified shortfalls in the areas of requirements specifications. Based on the outcomes of my assessment I am of the opinion that this shortfall is common for all UK HPR1000 C&I systems, and Assessment Finding AF-UKHPR1000-0034 (see sub-section 4.6.1) has been raised for the licensee to resolve issues with requirements management.

369. I identified the potential for signals from other C&I systems to affect the SAS and raised AF-UKHPR1000-0038 for this to be addressed by the licensee.

370. I also identified apparent shortfalls in the area of periodic testing and raised AF-UKHPR1000-0030 (see Section 175) for this to be resolved during site-specific stages of the project.

371. I found that the SAS safety case evidence did not always support the arguments and evidence, but that this is common across systems, and AF-UKHPR1000-0052 (see Section 4.11) has been raised.

4.6.2.4 Conclusion

372. In conclusion, I judge that sufficient information has been provided for a meaningful assessment of the SAS to be carried out that is sufficient for the purposes of GDA. Appropriate standards have been identified and standards compliance analysis has been performed. However, I have found that sufficient evidence has not always been provided to demonstrate how the standards clauses have been met. Similarly, I found that the safety case is not always adequately supported by evidence. As with the other UK HPR1000 systems, I found that the system requirements have not been clearly and completely established, and it I could not confirm that the intent of the system functions and properties has been met by the system design, and that relevant SAPs, such as EDR3, ESS.21, and EMT.7, have been satisfied. These issues have been taken forward as Assessment Findings.

4.6.3 Adequacy of the KDS [DAS]

4.6.3.1 Assessment

373. The PCSR (Ref. 3) and the BSCs for the overall C&I architecture (Ref. 44) and the KDS [DAS] (Ref. 101) state that the KDS [DAS] is the secondary means of protection under design basis fault conditions for frequent faults combined with a CCF of the primary means of protection, i.e. the RPS [PS] and SAS.

374. The architecture of the KDS [DAS] comprises three redundant and physically separated divisions to ensure no single failure results in the loss of safety functions. Interconnections between divisions and with other C&I systems are protected by electrical and optical isolation to ensure failures do not propagate. The system design incorporates features to ensure diversity, including equipment diversity, signal diversity and functional diversity, to reduce the likelihood of coincident failure of the KDS [DAS] and RPS [PS].

375. Given the fact that the hardware-based platform for the KDS [DAS] is only at the preliminary design stage (the assessment of which is detailed in sub-section 4.5.2 of this report), my assessment of the KDS [DAS] was limited to consideration of the functional and non-functional requirements of the system and the extent to which they demonstrate that the system will meet regulatory expectations.

System Requirements

376. I wanted to confirm that adequate system requirements have been identified for the KDS [DAS]. My assessment considered SAPs ESS.2, ESS.10 and ESS.11, relating to safety system specification, capability and adequacy, as well as IEC 61513 (Ref. 21) and was informed by relevant RP submissions, including:

- 'UK HPR1000 Fault Schedule' (Ref. 131).
- 'BSC of Diverse Actuation System' (Revision C) (Ref. 101).
- 'Safety Requirements of the Diverse Actuation System' (Revision E) (Ref. 189).
- 'Functional Requirements of the KDS [DAS]' (Revision C) (Ref. 223).
- 'KDS [DAS] System Requirements Specification' (Revision D) (Ref. 224).
- 'Technical Requirements Specification of the KDS [DAS] Platform' (Revision C) (Ref. 67).

377. My review of the SRS for the KDS [DAS] (Ref. 224) identified that functional requirements are broken down into three functional types; automatic actuation, manual actuation and interlock/permissive functions. Simple logic diagrams are provided to describe the automatic actuation and permissive functions. I sampled a number of functional requirements and judged that they were adequately specified for GDA and given the early stage of the system design.

378. I undertook a sample review of the fault schedule (Ref. 131) to understand how the KDS [DAS] functional requirements are derived from the fault analysis. I found that the safety function requirements listed in the fault schedule were traced through to the functional requirements specification (Ref. 223) with a unique 'safety function requirement code'. These requirements were then traced into the SRS (Ref. 224), although this was through reference to the tables where the functional requirements are specified, and there was no reference to the unique requirement code – in fact within the SRS individual requirements were given another unique identifier. I also noted that there were often differences between the functional descriptions in the fault schedule and the SRS. I have therefore concluded that, while it was possible to trace safety function requirements from the fault schedule into the SRS, this required a level of pre-existing knowledge of the generic UK HPR1000 design and I judge this to be a shortfall against SAP ESS.2. This shortfall is common across all C&I systems assessed within and has been taken forward by Assessment Finding AF-UKHPR1000-0034 (see sub-section 4.6.1).

Safety Properties

379. I sought to understand how the safety properties of KDS [DAS] have been derived, considering the following SAPs:

- EDR.1 Failure to safety;
- EDR.2 Redundancy, diversity and segregation;
- ESS.21 Reliability;
- ESS.23 Allowance for unavailability of equipment;
- ESS.25 Taking safety systems out of service.

380. My review of the BSC (Ref. 101) found that there were claims and arguments related to the safety properties of the system and that these were underpinned by references to evidential documents, including the functional requirements document (Ref. 223), safety requirements document (Ref. 189), SRS (Ref. 62) and technical requirements specification (Ref. 67). I judged the safety property claims to be credible.

381. My review of the SRS (Ref. 224) identified that these claims had been translated into a set of performance requirements for the KDS [DAS]. The document also provided a requirements traceability table that identifies the source of each requirement. I found

that several of the safety property/ performance requirements had been derived from international standards that are considered RGP.

382. I sampled the system requirements to seek confidence that the expectations of the SAPs were met. While I found evidence that satisfied SAPs (Ref. 2) EDR.2 and ESS.21, I found no requirements that considered the expectations of SAPs ESS.23 and ESS.25. Specifically, while requirements are specified to enable a single division of the system to be bypassed for testing or maintenance purposes, it was not clear how these functions would be governed in the event that one division is already unavailable. Given the preliminary design stage of the KDS [DAS] I consider that this is something that will be addressed as the design develops and hence I judge this to be a minor shortfall.

383. I also note that, in consideration of failure to safety, the KDS [DAS] actuation logic is 'energised-to-actuate'. The BSC claims that this configuration prevents spurious actuation of the KDS [DAS] from inhibiting plant operation. Despite this claim I judge the configuration of the logic as 'energised-to-actuate' to be a shortfall against the expectations of SAP EDR.1, in that a loss of power would mean that the safety functions could not actuate. I am of the opinion that resolution of this shortfall will depend on licensee design choices and hence I have raised an Assessment Finding for this to be addressed by the licensee.

AF-UKHPR1000-0040 – The licensee shall, during detailed design of the Diverse Actuation System, demonstrate that all reasonably practicable measures have been taken to ensure that the system to fails safely on loss of power.

384. My review of the 'Technical Requirements Specification for the KDS [DAS] Platform' (Ref. 67) found that the performance requirements specified in the SRS had been translated into a number of design requirements to be achieved by the Simple Hardware Platform. Traceability was provided through reference to the unique identifiers that had been assigned against each requirement in the SRS. Although little detail was provided on how the design requirements are to be implemented, given the preliminary design stage of the simple hardware platform I judge the level of detail provided to be reasonable.

4.6.3.2 Strengths

385. On the basis of the evidence sampled in my assessment of the KDS [DAS] design I judge that the proposed architecture is adequate for a Class 2 system. The system requirements are specified to a level which is suitable for the preliminary design stage and the relevant SAPs have been considered in the definition of performance requirements.

4.6.3.3 Outcomes

386. My assessment of the adequacy of the KDS [DAS] identified that the RP has not provided a suitable justification for how the actuation logic of the system supports the principle of failure to safety. This has been taken forward as Assessment Finding AF-UKHPR1000-0040

387. I also identified shortfalls in the traceability of requirements from the fault schedule into the system design; this is a common issue across all C&I systems and has been taken forward through Assessment Finding AF-UKHPR1000-0034 (see sub-section 4.6.1).

4.6.3.4 Conclusion

388. Based on the outcome of my assessment I judge that the RP has adequately demonstrated the adequacy of the KDS [DAS] in the context of GDA and that the expectations of SAPs EDR.2, ESS.10, ESS.11 and ESS.21 have been met.

389. I identified shortfalls against SAPs ESS.2 and EDR.1 and have raised Assessment Findings for these to be addressed by the licensee.

390. I also identified minor shortfalls against SAPs ESS.23 and ESS.25 which I expect to be addressed as part of normal business by the licensee.

4.6.4 Adequacy of the PSAS

4.6.4.1 Assessment

391. The BSC of the Plant Standard Automation System (Ref. 48) contains claims that the PSAS performs a range of FC3 (Category C) safety and non-classified functions to control reactivity, remove heat, and to confine radioactive material. I assessed the PSAS on the basis that this is a Class F-SC3 (Class 3) system performing FC3 (category C) safety functions. The PSAS is implemented using the HOLLiAS-N platform.

System Requirements

392. I wanted to confirm that adequate system requirements have been identified for the PSAS. My assessment considered a range of SAPs including ESS.10 and ESS.11 relating to capability and adequacy, as well as IEC 61513 (Ref. 21), and was informed by relevant RP submissions, including:

- ‘BSC of Plant Standard Automation System’ (Revision C) (Ref. 48).
- ‘UK HPR1000 Fault Schedule’ (Ref. 131).

393. The BSC of the Plant Safety Automation System (Ref. 48) describes a number of safety functions using a CAE structure. Based on my sampling, I judge this structure to be suitable to form the basis for argumentation for the PSAS.

394. I assessed the adequacy of the tracing of the requirements between the ‘BSC of the Plant Safety Automation System’ (Ref. 48) and the Fault Schedule (Ref. 131). I noted that PSAS functions are included in the fault schedule, for example for manual control of injection of borated water (REA-FFR-01-M41), and that this is referenced as an argument for claim C1.1.5-R2-3 in the BSC of Plant Standard Automation System (Ref. 48). I note that the primary function of the PSAS is to control the UKHPR1000 plant, and not to automatically act in response to a failure (the function described above is manual). In this respect the PSAS is primarily a potential initiator of faults which are detected and terminated by the actions of safety systems. I am satisfied, based on the sample of requirements I assessed, that there is adequate linkage between the ‘BSC of Plant Standard Automation System’ and the fault schedule (Ref. 131).

Application of Relevant Standards and Demonstration of Production Excellence

395. I wanted to confirm that appropriate standards have been identified for the development of the PSAS as described in SAPs ECS.3 and ESR.5. My assessment was informed by relevant RP submissions, including:

- ‘Comparison of UK HPR1000 PSAS and KIC [PCICS] with IEC 61513’ (Ref. 92).
- ‘Demonstration of Production Excellence for PSAS and KIC [PCICS]’ (Revision B) (Ref. 225).

- ‘Comparison Analysis of PSAS and KIC [PCICS] with IEC 62138’ (Ref. 93).
- ‘PSAS System Requirements Specification’ (Revision D) (Ref. 61).
- ‘BSC of Plant Standard Automation System’ (Revision C) (Ref. 48).
- ‘Suitability Analysis Report of the Selected Platform Applicability to the PSAS & KIC [PCICS] System Requirements’ (Ref. 226).

396. I was satisfied that appropriate high-level standards had been identified in the ‘PSAS System Requirements Specification’, e.g. IEC 61513 (Ref. 21), IEC 62138 (Ref. 22), and IEC 61226 (Ref. 18).

397. I observed that in the ‘BSC of Plant Standard Automation System’ (Ref. 48), claim C1.1.1.5, argument A1 states that commercial hardware development processes are used, but does not specify what these are. The focus of this clause appeared to be on reliability and testing, rather than specific engineering techniques to achieve both suitable reliability and integrity. Similarly, argument A2 related to self-diagnosis, but this did not reference standards.

398. I consider the lack of demonstration that the PSAS hardware design is adequate through the application of appropriate standards to be a shortfall that should be tracked to resolution. I have therefore raised an Assessment Finding for this to be addressed by the licensee.

AF-UKHPR1000-0041 – The licensee shall ensure that all relevant standards are selected and applied to the design of the Plant Standard Automation System, including hardware standards, and a demonstration is provided that the design approach is commensurate to the required reliability and integrity.

399. I elected not to assess the detailed evidence supporting the claims that relevant standards have been complied with by the PSAS during GDA Step 4 due to the modest classification of this system, so I cannot draw a conclusion as to whether these standards have been met by the PSAS design. I note that the PSAS design will be further developed during site-specific stages of the project and it is my expectation that evidence to demonstrate that relevant standards have been complied with will be available for assessment during site-specific stages of the project. This is addressed by Assessment Finding AF-UKHPR1000-0024 (see Section 41).

400. I considered the suitability of the PE evidence for the PSAS by assessing the document ‘Demonstration of Production Excellence for the PSAS and KIC [PCICS]’, Revision B (Ref. 225). This describes the lifecycle of the design of the PSAS, showing how the plant requirements are translated into system requirements, and how these system requirements are used to generate the PSAS system design, including software requirements and V&V activities. I judge this to be an appropriate approach, but some of the argumentation relating to the suitability of the approach is based on multiple previous applications of the HOLLiAS-N platform without any reference to supporting evidence. General claims that the system design approach has been successful in the past provide limited confidence that the same approach will be effective in all future circumstances. It is a UK regulatory expectation that potential sources of faults in system design be identified and for supporting evidence to show how the design approach is effective to prevent these resulting in an incorrect system design.

401. Section 6.2 of the submission ‘Demonstration of Production Excellence for the PSAS and KIC [PCICS]’, Revision B (Ref. 225) acknowledges that shortfalls have been identified in the PE approach for the FirmSys platform, and that the RP has performed an analysis to identify if similar shortfalls are also present in the PSAS system design PE evidence. This identified shortfalls in a number of areas including design review and verification records, system security plan, software configuration information, and system requirements specification and traceability. A number of compensating

measures have been identified using a similar approach to that developed to address the FirmSys PE evidence shortfalls, and it is claimed that these can be applied within the timescale of a typical build project. The evidence submitted in GDA was insufficient for me to make a judgement on the suitability of the proposed CMs.

402. The shortfalls identified in the PSAS PE evidence, and the associated CMs, are similar to those identified for the RPS [PS] and SAS. This issue will therefore be addressed by Assessment Finding AF-UKHPR1000-0035 (see sub-section 4.6.1).

Safety Properties

403. I assessed the suitability of the PSAS system design by sampling specific areas, using relevant SAPs and TAGs and standards to guide my assessment. I concluded that:

- It is difficult to determine that regulatory expectations expressed in EDR.1, have been comprehensively addressed in the PSAS design. Claim C2.1.6.1 states that "The design of PSAS includes redundancy and other features necessary to provide tolerance to failure.", and a number of measures to detect errors and respond to failures in the HOLLiAS-N platform are described. However, it is not clear that all potential sources of failure and errors have been considered at the system level, as the supporting evidence is focused on system functional and performance requirements. It is my opinion that further work will be necessary during site-specific stages of the project to integrate the safety case evidence with the claims and arguments that fail safe behaviour has been achieved, so that the PSAS design can be fully substantiated, and that the fail-safe behaviour of the PSAS can be demonstrated. I judge this to be a minor shortfall.
- Redundancy, diversity and separation (EDR.2) have been considered in the PSAS design. For example, measures to restrict the effects of failures are deployed using redundancy. It is not evident that the PSAS includes diversity, although I note diversity is generally provided in different layers of protection and is often not necessary to deploy diversity to achieve adequate resilience to faults within a single layer of protection such as the PSAS. Argument A1 relating to claim C2.1.6.2 states that the redundant divisions of the PSAS are separated, and provides some information on how this is achieved, e.g. physical separation of redundant cabinets and cables. I am content that this is adequate for GDA Step 4, although I note that further identification of hazards and demonstration of the resistance of PSAS to these will be necessary during detailed design and substantiation. This is addressed by Assessment Finding AF-UKHPR1000-0029 (see Section 4.3).
- Common cause failure (EDR.3) arising from the PSAS has been considered in relation to the potential for this to cause spurious actuation of plant items controlled by the PSAS, and for this to place safety demands on other systems (claim 2.1.6.6, A1). It has been demonstrated that these demands can be managed through the initiation of safety systems to prevent unacceptable consequences (see para 154). However, I observe that it is undesirable to place demands on safety systems where this can be avoided, and that it may be reasonably practicable to implement additional measures to prevent spurious actuation arising from the PSAS. My expectation is that further measures to prevent spurious actuation arising from the PSAS will be considered as the design is developed during site-specific stages of the project, and that these will be implemented where it is reasonably practicable to do so. This is captured by AF-UKHPR1000-0037 (see sub-section 4.6.1).

4.6.4.2 Strengths

404. During GDA Step 4 the RP has improved the PSAS safety case structure and content. This has resulted in greater clarity of intent and better linked the evidence to the claims

and arguments. There is adequate linkage between the fault schedule and the PSAS safety case.

4.6.4.3 Outcomes

405. My assessment identified that, in general, suitable standards has been referenced in relation to the PSAS. However, I noted that no hardware design standard has been referenced; AF-UKHPR1000-0041 has been raised to address this.

406. I am satisfied that there is adequate linkage between the 'BSC of Plant Standard Automation System' (Ref. 48) and the fault schedule (Ref. 131), also that redundancy has been considered in the design. I also note that measures to control common cause failure have been considered in relation to the potential for this to cause spurious actuation of plant items controlled by the PSAS.

407. Shortfalls in the area of PSAS PE were identified during GDA step 4, and these have common causes for all systems, and for which AF-UKHPR1000-0037 (see sub-section 4.6.1) has been raised.

4.6.4.4 Conclusion

408. In conclusion, I judge that sufficient information has been provided for a meaningful assessment of the PSAS to be carried out that is sufficient for the purposes of GDA. Appropriate standards have been identified (except in the case of a hardware design standard) and standards compliance analyses have been performed. As with the other UK HPR1000 systems I found that the system requirements have not been clearly and completely established, and it is therefore difficult to confirm that the intent of the system functions and properties has been met by the system design, and that relevant SAPs, such as ECS.3, ESR.5, and ESS.27, have been satisfied. These issues have been taken forward as Assessment Findings.

4.6.5 Adequacy of the KIC [PCICS]

4.6.5.1 Assessment

409. The 'BSC of Plant Computer Information and Control System' (Ref. 49) states that the KIC [PCICS] system performs a range of safety and non-classified functions to control and monitor F-SC3 and NC reactor systems, and to monitor F-SC1 and F-SC2 systems. The functions performed by the KIC [PCICS] are:

- information display;
- manual control of FC3 and non-classified functions;
- management of alarms;
- display of computer-based procedures;
- recording and display of events; and
- automatic diagnosis.

410. I assessed the KIC [PCICS] on the basis that this is a Class F-SC3 (Class 3) system performing FC3 (category C) safety functions. The KIC [PCICS] is implemented using the HOLLiAS-N platform.

System Requirements

411. I wanted to confirm that the adequate system requirements have been identified for the KIC [PCICS]. My assessment considered a range of SAPs including ESS.10 and ESS.11 relating to capability and adequacy, as well as IEC 61513 (Ref. 21), and was informed by relevant RP submissions, including:

- ‘BSC of Plant Computer Information and Control System’ (Revision D) (Ref. 49).
- ‘Comparison of UK HPR1000 PSAS and KIC [PCICS] with IEC 61513’ (Ref. 92).
- ‘Demonstration of Production Excellence for PSAS and KIC [PCICS]’ (Revision B) (Ref. 225).
- ‘Comparison Analysis of PSAS and KIC [PCICS] with IEC 62138’ (Ref. 93).
- ‘KIC [PCICS] System Requirements Specification’ (Revision D) (Ref. 62).
- ‘Suitability Analysis Report of the Selected Platform Applicability to the PSAS & KIC [PCICS] System Requirements’ (Ref. 226).
- ‘Design Specification of the KIC [PCICS]’ (Revision D) (Ref. 68).

412. The ‘BSC of Plant Computer Information and Control System’ (Ref. 49) presents a CAE structure for the functional and non-functional properties of the KIC [PCICS]. The claims cover reliability, function performance requirements, resistance to hazards, etc. However, I noted that it is not necessarily clear on what principle the arguments are based. For example, claim C1.4.6.1 states that “The time related to HMI of the KIC [PCICS] meets the relevant ergonomic requirements.”, but the supporting argument A1 simply lists a series of target response times without unique identification, identifying the source of these, or providing a demonstration that they are adequate. I also noted that the evidence sources are not specifically identified, so it is difficult to determine exactly where the evidence is that is intended to support the arguments and claims. This limitation is similar to that seen in the safety cases for other systems. My expectation is that this will be improved as the KIC [PCICS] design is developed during site-specific stages of the project.

413. The KIC [PCICS] system requirements (Ref. 62) are uniquely identified and include both functional and non-functional requirements, e.g. [KIC-SDS-0006] “The KIC [PCICS] can store the event data being exactly consistent with the correct time stamp and queue the events chronologically.” and [KIC-SDS-0094] “The KIC [PCICS] equipment is seismically qualified…”. In ‘Suitability Analysis Report of the Selected Platform Applicability to the PSAS & KIC [PCICS] System Requirements’ (Ref. 226), these requirements are supplemented with text that describes how those requirements have been met, but not why they are necessary, or why they are adequate. I observe that many requirements are not precisely stated, and appear to be a justification that the system already designed is adequate, not to elicit and substantiate system functions and properties. I consider this shortfall to be similar to that identified during the rest of my assessment of the UKHPR1000 C&I systems, and has been taken forward by Assessment Finding AF-UKHPR1000-0034 (see sub-section 4.6.1) so it is not discussed further in this section.

Application of Relevant Standards and Demonstration of Production Excellence

414. I wanted to confirm that appropriate standards have been identified for the development of the KIC [PCICS], as set out in SAPs ECS.3 and ESR.5.

415. It is stated in the KIC [PCICS] SDS (Ref. 69) that the engineering lifecycle has been developed in accordance with IEC 61513 (Ref. 21), and references to IEC 61513 clauses are made in the KIC [PCICS] SRS (Ref. 62). The document ‘Comparison of UK HPR1000 PSAS and KIC [PCICS] with IEC 61513’ (Ref. 92) provides a more detailed review of the requirements of IEC 61513 clauses. However, limited evidence is offered to demonstrate that these clauses have been met. Similarly, other standards are referenced, but insufficient detail was provided during GDA to confirm these have been satisfied. This has been taken forward as part of Assessment Finding AF-UKHPR1000-0024 (see Section 41).

416. Similarly, I note the submission ‘Comparison Analysis of PSAS and KIC [PCICS] with IEC 62138’ (Ref. 227) references individual IEC 62138 (Ref. 22) clauses and a

description of the general approach to meeting the requirements of that clause, but does not reference specific evidence to demonstrate that the intent of each clause of IEC 62138 has been achieved by the approach described. This is the same shortfall as that identified in my assessment of the PSAS and other systems. My expectation is that this will be improved as the KIC [PCICS] design is developed and documented during site-specific stages of the project. This is addressed by Assessment Finding AF-UKHPR1000-0024 (see Section 41).

417. I observe that sub-section 5.3.3.1 of the submission KIC [PCICS] SRS (Ref. 62) describes the potential faults that may occur with the KIC [PCICS] (detectable and non-detectable faults), and the measures to address these such as self-monitoring, monitoring using tools, “periodic check”, etc. However, there does not appear to have been a detailed consideration of the sources of potential faults, the potential consequences of these, or the suitability of the measures described. It is therefore not possible to determine the adequacy of the proposed measures, or whether additional measures may be necessary. In particular, it is not possible to determine if changes to the design of the system may be required to adequately control risks arising from system faults. It is essential that this is reflected in the system requirements, but at present there appears to be no mechanism to do this, e.g. hazard identification and consequence analysis of the KIC [PCICS]. I consider this to be a shortfall that requires tracking to resolution and have therefore raised this as Assessment Finding AF-UKHPR1000-0042 (see below).

418. I considered the suitability of the PE evidence for the KIC [PCICS] by assessing the document ‘Demonstration of Production Excellence for the PSAS and KIC [PCICS]’ (Ref. 225). This describes the lifecycle of the design of the KIC [PCICS], showing how the plant requirements are translated into system requirements, and how these system requirements are used to generate the system design, including software requirements and V&V activities. This generally appears to be an appropriate approach, but some of the argumentation relating to the suitability of the approach is based on multiple previous applications of the HOLLiAS-N platform without any reference to supporting evidence. I noted that general claims that the system design approach has been successful in the past provide only limited confidence that the system design approach will be effective in all circumstances in the future. It is a UK regulatory expectation that potential sources of system design fault be identified and for supporting evidence to show how the system design approach is effective to prevent these resulting in an inadequate system design.

419. Section 6.2 of the submission ‘Demonstration of Production Excellence for the PSAS and KIC [PCICS]’ (Ref. 225) acknowledges that shortfalls have been identified in the PE approach for the FirmSys platform, and the RP has performed an analysis to identify if similar shortfalls are also present in the KIC [PCICS] system design PE. This identified shortfalls in a number of areas including design review and verification records, system security plan, software configuration information, and system requirements specification and traceability. A number of compensating measures have been identified using a similar approach to that developed for the FirmSys PE, and it is claimed that these can be applied within the timescale of a typical build project. The evidence submitted in GDA was insufficient for me to make a judgement on the suitability of the proposed CMs.

420. The shortfalls identified in the KIC [PCICS] PE evidence, and the associated CMs, are similar to those identified for the other C&I systems. This issue will therefore be addressed by Assessment Finding AF-UKHPR1000-0035 (see sub-section 4.6.1).

421. The shortfalls identified and associated CMs are similar to those identified for the FirmSys platform, and I don’t consider it necessary to raise these separately, other than to note that this will require additional resource to resolve beyond that already identified for the FirmSys platform.

Satisfaction of Safety Claims

422. The 'BSC of Plant Computer Information and Control System' (Ref. 49) presents a top-level claim that the KIC [PCICS] provides FC3 functions to maintain core reactivity control (C1.1.7-R1), and sub claims C1.1.7-R1-1 "The KIC [PCICS] provides the Reactor Coolant System RCP [RCS] average temperature control function to maintain core reactivity control." and C1.1.7-R1-2 "The KIC [PCICS] provides reactor power control function to prevent unacceptable core thermal power.". However, the arguments for both sub claims indicate that the Rod Position Indication and Rod Control System (RPICS) is out of GDA scope. For this reason I have not assessed this system, or what KIC [PCICS] faults could affect it, with what consequences. However, in my opinion, it is feasible that a KIC [PCICS] fault could affect this system and result in the reactor operating at an incorrect power level. This is a potentially significant deviation from normal operation, which could affect the safety of the reactor. I consider the importance of this to be such that an Assessment Finding is necessary to ensure this is tracked during site-specific stages of the project.

AF-UKHPR1000-0042 – The licensee assess the nuclear safety risks arising from incorrect operation of the Plant Computer Information Control System impacting the Rod Position Indication and Rod Control System and implement any reasonably practicable measures required to those risks.

4.6.5.2 Strengths

423. During GDA Step 4 the RP has made improvements to the KIC [PCICS] safety case structure and content. This has resulted in greater clarity of intent and better linked the evidence to the claims and arguments.

4.6.5.3 Outcomes

424. My assessment has identified shortfalls in the areas of requirement specifications, and the evidence to support the safety case. This is also relevant for other UK HPR1000 C&I systems and has been taken forward by Assessment Finding AF-UKHPR1000-0034 (see sub-section 4.6.1).

425. Shortfalls in the area of KIC [PCICS] PE were identified during GDA step 4, and these have common causes for all systems, and for which AF-UKHPR1000-0035 (see sub-section 4.6.1) has been raised.

426. I have also identified a potential concern relating to the KIC [PCICS] control of the Rod Position Indication and Rod Control System (RPICS), and this is the subject of AF-UKHPR1000-0042.

4.6.5.4 Conclusion

427. In conclusion, I judge that sufficient information has been provided for a meaningful assessment of the KIC [PCICS] to be carried out that is sufficient for the purposes of GDA. Appropriate standards have been identified and standards compliance analyses have been performed. As with the other UK HPR1000 systems I found that the system requirements have not been clearly and completely established, and it is therefore difficult to confirm that the intent of the system functions and properties has been met by the system design, and that SAPS such as EDR.1, EDR.2 and ESS.17, have been satisfied. I have raised AF-UKHPR1000-0042 relating to potential hazards arising from its failure or faulty operation of the KIC [PCICS], considering its functionality in relation to the operation of the RPICS. My expectation is that further work to establish the KIC [PCICS] requirements, and to provide evidence to demonstrate these have been met will be carried out during site-specific stages of the project.

4.6.6 Adequacy of the KDA [SA I&C]

4.6.6.1 Assessment

428. The KDA [SA I&C] system is used during a severe accident to display the reactor status and communicate this to other systems, and to control severe accident plant items. This system is classified as F-SC3 (Class 3) and is based on the SpeedyHold platform.

429. I assessed the adequacy of the Severe Accident I&C system (KDA [SA I&C]) to meet UK regulatory expectations, in particular SAPs ESS.18, ESS.21, and ESR.7. My assessment was primarily based on the following documents:

- 'BSC of Severe Accident I&C System' (Revision C) (Ref. 102).
- 'KDA [SA I&C] System Requirements Specification' (Revision D) (Ref. 63).

430. I identified a number of apparent shortfalls in these documents in relation to the suitability of the proposed design to meet the claims being made, and issued RQ-UKHPR1000-1416 (Ref. 109) to raise concerns in a number of areas, including:

- The lack of clarity on the sources of requirements to establish the KDA [SA I&C] system requirements, and the completeness of these.
- The digital communications between the two KDA [SA I&C] channels, and between the KDA [SA I&C] system and other C&I systems, present a risk that faults or failures could prevent the correct operation of the KDA [SA I&C] system. Also, the lack of clarity on the detailed system architecture.
- The management of alarm set points.
- The potential for manual control functions to be prevented from operating due to interlocks or software faults, or spurious actuator demands to be generated.
- Potential lack of information of the state of the plant during a severe accident due to incorrect or misleading indications arising from hardware or software faults.

431. The response to RQ-UKHPR1000-1416 (Ref. 109) provided additional information and where necessary indicated how each area should be resolved:

- Some sources of requirements were identified, but a number of additional requirements were also identified.
- A more detailed system architecture diagram was provided. It was proposed that the digital communications between KDA [SA I&C] channels should be removed, and that digital communications with other I&C systems would either be removed or changed to one way communication from the KDA [SA I&C] system to other systems.
- The arrangements for the management of alarm set points were described.
- Interlocks were removed from the manual control functions and these are hardwired directly from the non software-based controls to the actuator, via the CIM where necessary. One exception is the annulus ventilation system EDE [AVS] for which there appears to be no significant detriment if interlocks prevent operation or from spurious actuation.
- The majority of the indications are of the 'conventional' type, not relying on software. However, the core outlet temperature indication relies on software to calculate average sensor inputs, and the measures to detect and respond to failures are described.

432. The response to the RQ also stated that the 'KDA [SA I&C] System Requirements Specification' would be updated to reflect the response to the RQ. I reviewed Revision E of this document (Ref. 64) and was satisfied that the RQ response had been incorporated.

433. I assessed the response to RQ-UKHPR1000-1416 (Ref. 109) and concluded:

- The sources of requirements for the KDA [SA I&C] system appear to be wide-ranging, but don't appear to be based on any higher level principles (such as nuclear safety, security and environmental principles). For this reason it is difficult to determine the suitability of the KDA [SA I&C] requirements when considering the higher level plant design objectives, or whether all requirements have been identified. This is the same finding as that identified for other C&I systems, and has been taken by Assessment Finding AF-UKHPR1000-0034 (see sub-section 4.6.1).

- The more detailed KDA [SA I&C] architecture diagram provides sufficient information, and there is now no interconnection shown between the redundant channels. This means that a failure in one channel cannot directly prevent the correct operation of the other channel, satisfying SAP ESS.18.

- However, I note that the removal of the connection between channels has the potential to affect operability in the event of a failure (e.g. each server will only contain information relating to the channel to which it is connected), but the potential consequences do not appear to have been identified. I consider this to be because the requirements of the KDA [SA I&C] system have not been fully established, and this is the same point as described elsewhere. Also, digital communication between the KDA [SA I&C] system and other C&I systems is now one-way only from the SA I&C system. This significantly reduces the potential for faults or failures in other systems to propagate to the KDA [SA I&C] system, and in my opinion satisfies ESR.7.

- The alarm system settings can be modified by a maintenance tool, and a number of mechanisms to prevent unauthorised or unexpected modification of alarm settings are described. However, the RQ response acknowledges that there is no explicit requirement for the alarm settings to be tested, and such a requirement is identified. I consider this to be another case of a shortfall in requirements, and whilst the proposed arrangements appear to be appropriate, the shortfall in requirements means that it is not clear that the risks relating to the alarm system are adequately managed.

- The use of a hardwired connection between the conventional controls and the actuators and the removal of interlocks ensures that the risk of an operator being unable to successfully operate safety equipment, and the risk of spurious actuation of safety equipment is reduced. I judge that this satisfies SAP ESS.21. In the case of the annulus containment system there appears to be no significant detriment arising from the interlocks or potential spurious actuation of this.

434. I consider that it is appropriate that all but one of the indicators of the plant state use technology that does not rely on software. The exception, core outlet temperature (COT), relies on software to perform both fault identification and averaging functions, and I judge this is beneficial because this allow faults to be identified and alarmed to the operator immediately these occur. I also note that there are other indications, in addition to the COT, that allow a severe accident to be identified, such as a high containment dose rate. The operators are thus not solely dependent on the COT to detect the onset of a severe accident, to determine its severity, or to determine whether actions taken are having the expected effect on the plant.

435. The modification to the KDA [SA I&C] system was formalised as M89 (Ref. 200), and a revised ‘KDA [SA I&C] System Requirements Specification’ (Ref. 63), and the ‘Independence Analysis of I&C Systems’ (Ref. 142) were submitted. I have confirmed

that the improvements identified in the response to RQ-UKHPR1000-1416 (Ref. 109) have been incorporated into these documents. I also confirmed that improvements have been made to the claims, arguments, and evidence presented in Revision C of the 'BSC of Severe Accident I&C System' (Ref. 102). For example, new claims have been added to address cyber security (C2.5.1.4) and spurious actuation (C2.5.1.5).

436. I observe that the modifications made to the KDA [SA I&C] system during GDA Step 4 (Ref. 200), and documented in the 'BSC of Severe Accident I&C System' (Ref. 102) have significantly reduced the influence of the SpeedyHold platform on the KDA [SA I&C] system. Specifically, the SpeedyHold platform no longer performs interlock and control functions for the majority of severe accident functions; these functions are now hardwired from the conventional (non computer-based) controls to the actuator or CIM. Therefore, a SpeedyHold fault can neither prevent the actuation of a function, nor spuriously cause a function to actuate. Similarly, the majority of the KDA [SA I&C] indicators use conventional components that are directly connected to sensors. Thus a fault in the SpeedyHold platform or the KDA [SA I&C] system will not prevent the correct indication of the plant state. An exception to this is the core outlet temperature (COT) indication that requires additional averaging and fault detection, for which the SpeedyHold platform is used. However, I am content with this because there are other means by which the plant state and success of actions can be determined.

437. Whilst improvements to the KDA [SA I&C] system are adequate for the purposes of GDA Assessment Finding AF-UKHPR1000-0034 (see sub-section 4.6.1) has been raised for the requirements for this system (and other systems) to be further elicited and refined. It should be noted that improvements to the requirements may identify that further design improvements are necessary to ensure that risks have been reduced so far as is reasonably practicable.

438. I also note that the cyber security protection cabinet is still incorporated into the KDA [SA I&C] design, despite the communication link being modified to a unidirectional communication link from the KDA [SA I&C] to the PSAS and KCC [NAEMS]. The introduction of this one way link will mean that there can be no cyber security threat to the KDA [SA I&C] system by this route, and therefore this equipment would appear to be unnecessary within the KDA [SA I&C] system. However, because the requirements for the KDA [SA I&C] system have not been fully established during GDA it is not possible to determine whether there is still a role for this equipment.

4.6.6.2 Strengths

439. The RP has addressed concerns raised by ONR during GDA step 4 and has modified the proposed KDA [SA I&C] design. This has resulted in greater resilience to faults that could prevent operation of SA plant equipment, or spurious actuation that could inadvertently actuate plant equipment and which could present a hazard to the safety of the plant.

4.6.6.3 Outcomes

440. During GDA the RP has identified and resolved some gaps in the KDA [SA I&C] requirements, modified the KDA [SA I&C] design, and improved the clarity and content of the KDA [SA I&C] documentation. This has been sufficient for the purposes of GDA, and has established that further work will be necessary during site-specific stages of the project. In particular, this includes determining a clear set of requirements which ensures that the functional and non-functional properties of the KDA [SA I&C] system are clearly identified, and will allow a demonstration to be made that risks relating to the KDA [SA I&C] can be reduced, so far as is reasonably practicable.

4.6.6.4 Conclusion

441. In conclusion, I judge that sufficient information has been provided for a meaningful assessment of the KDA [SA I&C] system to be carried out that is sufficient for the purposes of GDA. Design changes have been made in response to ONR challenge during GDA step 4, and these have improved the resilience of the system to software and hardware faults based upon the general role of a severe accident system. However, until comprehensive requirements are established for the KDA [SA I&C] system, it will not be possible to determine the adequacy of the system , or that relevant SAPs, such as EDR1, ESS.18, and ERL.2, have been satisfied. Assessment Finding AF-UKHPR1000-0034 (see sub-section 4.6.1) has been raised for the requirements of all C&I systems, including the KDA [SA I&C] system to be established.

4.7 Independent Confidence Building Measures for all systems

4.7.1 Assessment

442. I assessed the suitability of the proposed ICBMs for each of the relevant systems, namely the RPS [PS] and SAS, both based on the FirmSys platform, the PSAS and KIC [PCICS], both based on the HOLLiAS-N platform, and the KDA [SA I&C], based on the SpeedyHold platform. It should be noted that no ICBMs are specified for the Class 2 KDS [DAS] as this relies on a hardwired platform which does not use microprocessors or complex configurable hardware logic devices, such as FPGAs, for the delivery of safety functions. The KDS [DAS] does contain complex components in the monitoring and test modules, but it has been demonstrated during GDA step 4 that these do not perform safety functions directly, and that they will not interfere with safety functions. For my assessment of this, see sub-section 4.6.3 of this report. For this reason I have not considered ICBMs for the KDS [DAS] system.

443. I noted that the intent of applying ICBMs is that these provide confidence that the PE activities have been effective in producing a system that is adequately engineered, and that this can demonstrated.

444. The selection and application of ICBMs for systems containing complex devices such as microprocessors and HPDs is governed by UK RGP and, in particular, relevant international standards and guidance such as IEC 61508 (Ref. 20). Guidance for ONR inspectors in respect of the adequacy of ICBMs is described in SAP ESS.27 and NS-TAST-GD-046. When assessing the suitability of the ICBMs I have considered the classification of the systems, and the reasonable practicability of applying them. It should be noted that the reasonable practicability of applying certain ICBMs such as source code comparison and statistical testing for Class 1 systems has been established in the UK.

445. ICBMs cannot be applied until the system designs have been completed. Therefore, my expectation is not that ICBMs should be deployed during GDA, but that it should be determined which ICBMs will be deployed for each system, and that this is feasible.

446. I was concerned during GDA Step 4 that a coherent strategy did not appear to have been established by the RP for the application of ICBMs across all the UK HPR1000 systems. I therefore raised RO-UKHPR1000-0057 'Independent Confidence Building Measures for Complex Control and Instrumentation Systems' (Ref. 40) because I considered it important that the RP develop a common approach to the application of ICBMs for all UK HPR1000 systems that use complex logic to perform safety functions. My assessment of RO-UKHPR1000-0057 is documented in an assessment note (Ref. 228) and is summarised in the below paragraphs. The RO specified the following two actions:

- to develop a strategy for implementing ICBMs, considering appropriate factors and UK RGP; and
- to demonstrate the feasibility of applying the ICBMs

447. The RP provided a resolution plan (Ref. 229) and subsequently submitted a number of documents setting out how ICBMs would be applied to the UK HPR1000 systems:

- 'Strategy for Conducting ICBMs Activities for RPS [PS]' (Revision C) (Ref. 211).
- 'Strategy for Conducting ICBMs Activities for SAS' (Revision C) (Ref. 222).
- 'Strategy for Conducting ICBMs Activities for PSAS and KIC [PCICS]' (Revision C) (Ref. 230).
- 'Strategy for Conducting ICBMs Activities for KDA [SA I&C] (Revision C)' (Ref. 231).
- 'Feasibility Study Report for Static Analysis of Protection System' (Ref. 232).
- 'Feasibility Study Report for Source Code Comparison of Protection System' (Ref. 233).
- 'Feasibility Study Report for Statistical Testing of Protection System' (Revision B) (Ref. 234).

448. My assessment of these submissions revealed that they contain some common sections with identical information. I therefore assessed the common sections first:

449. I found the sections on objectives and safety case structure to be acceptable, for example, by noting that the ICBM techniques and measures should be independently conducted and dissimilar to the PE and setting out a structure that supports the development of a CAE-based safety case. The section on the general approach to ICBMs identifies suitable standards according to the class of the system, and sets out a series of PE review activities, according to the classification of each system.

450. I noted that independent review of developer supplied verification and testing evidence for F-SC2 systems, and independent review of type testing at F-SC3, are not specified. I requested clarification for this and other points in RQ-UKHPR1000-1602 (Ref. 109). The RP response indicated that a sample-based review will be implemented for F-SC2 (Class 2) systems based on the requirements of IEC 62138 (Ref. 22), and that review of type testing at F-SC3 (Class 3) will be performed where type testing results exist. The RP also clarified what organisational features are necessary for independence, confirmed static analysis would include compliance analysis/formal proof for systems with a claimed reliability of 10^{-4} pfd, and that control flow, data analysis, information flow and semantic analysis would be performed for systems with a claimed reliability of 10^{-3} pfd. The RP indicated that at the time of GDA, source code comparison is not considered for 10^{-3} pfd systems, but with future tool development and automation this may become reasonably practicable at the point of deployment. I consider the approach to ICBMs to be acceptable at this time but note that technical developments may mean that other ICBM techniques may be available and reasonably practical at the time they are wanted. I confirm that the responses have been incorporated into the ICBM strategy documents for each significant C&I system (Ref. 211) (Ref. 222), (Ref. 230) and (Ref. 231).

451. I assessed the suitability of the ICBM document for each system, as described below.

4.7.1.1 RPS [PS] ICBM Strategy

452. The 'Strategy for Conducting ICBMs Activities for RPS [PS]' (Ref. 211) provides information specific to the RPS [PS], such as the overall development approach, including verification activities and the development of application software. I noted that it identified that it is not currently possible to demonstrate the correctness of the internal configuration of HPD's, but that an analysis will be performed during site-specific stages of the project to assess the potential consequences of misconfiguration,

and where necessary, for mitigation to be developed. In addition, it is proposed that on-chip testing will be performed to provide confidence in the HPD configuration. I also note that where a shortcoming in the independent PE review of the platform or of the application software is identified, this will be reported to an independent sentencing panel for resolution. I consider this to be good practice.

453. During my assessment I noted that the PS-SCID control and display terminal has a reliability target less than that of the main RPS [PS] at 10^{-3} pfd, and that compliance analysis and formal proof is therefore not considered as an ICBM for this. My understanding is that it has been demonstrated during GDA that a failure of the PS-SCID will not lead to a safety consequence, and Section 500 of this report provides more information on this.

454. The submission 'Feasibility Study Report for Static Analysis of Protection System' (Ref. 232) describes static analysis techniques that could be applied to the RPS [PS], including analysis of control flow, data use, information flow, code semantics, etc. These are all valuable techniques that, when applied appropriately, can identify design and PE execution shortfalls. The report also sets out the aims of applying static analysis to the RPS [PS], in particular that the RPS [PS] software can be directly traced back to safety functional requirements, and has appropriate integrity. These aims are clearly stated and appropriately linked to techniques to achieve each aim.

455. The report sets out what input documentation is required to enable static analysis techniques to be successfully applied, and describes in outline the RPS [PS] application software development process. A good understanding of the documentation requirements is demonstrated. The report also sets out what resources and capabilities are needed for a successful static analysis programme to be organised and run, including planning, work instructions, competency arrangements, and scheduling. The identified resources and capabilities demonstrate a good understanding of the amount of effort and knowledge required.

456. Whilst I was satisfied with the proposed approach to the application of static analysis to the RPS [PS] set out in this report, my wider C&I assessment identified concerns in relation to the suitability of information available to perform static analysis on the RPS [PS]. Specifically, my assessment of the FirmSys platform production excellence documentation identified significant documentary shortfalls. I raised RO-UKHPR1000-0059 (Ref. 40) during GDA Step 4 for the RP to assess the adequacy of the FirmSys PE documentation. The consequent self-assessment by the RP identified significant and wide-ranging shortfalls in the adequacy of the FirmSys and associated RPS [PS] documentation. Assessment Findings AF-UKHPR1000-0031 (see sub-section 195) and AF-UKHPR1000-0034 (see sub-section 4.6.1) have been raised for the identified shortfalls to be addressed during the detailed design stage.

457. The submission 'Feasibility Study Report for Source Code Comparison of Protection System' (Ref. 233) describes the requirements for effective source code comparison (SCC) of the RPS [PS] to be carried out. SCC can show that the software (the executable image) implemented on the RPS [PS] exactly matches the source code, and that no errors have been introduced by design manipulation, including any software tool such as a compiler. This report clearly describes the overall aims of SCC, the necessary inputs, the programme, and the competences necessary for individuals carrying out the comparison work.

458. It is necessary for the RPS [PS] source code to be suitable for analysis and the report states that the system developer responses to a questionnaire on the RPS [PS] language constructs indicate that the source code is likely to be analysable, and a pilot study is proposed to confirm this. I judge this approach to be appropriate, as this allows any potential challenges to be identified early. My expectation is that this work will be progressed sufficiently early in site-specific stages of the project to confirm the

feasibility of this approach, or to develop an approach that will enable SCC to be achieved.

459. The feasibility of statistical testing (ST) is described in the document 'Feasibility Study Report for Statistical Testing of Protection System' (Ref. 235). This describes what preparation for ST will be needed, the test equipment configuration, how STs will be built to reflect operational profiles as closely as possible, how the results will be sentenced, and limitations. It is stated that approximately 46,000 statistical tests of the RPS [PS] will be performed. In respect of limitations, it is noted that certain parts of the RPS [PS] such as the HMI operate in continuous mode, and therefore statistical testing is not suitable for these parts of the system. I concur that at present ST is only applicable to demand mode systems, although I note that future research may establish a ST approach that is suitable for continuous mode systems.

460. I assessed this document and raised RQ-UKHPR1000-1367 (Ref. 109) to clarify a number of areas including what modifications would trigger the need to repeat ST, and the suitability of the proposed approach to simulate inputs from other RPS [PS] divisions. The response to these queries was acceptable, in that the need to repeat ST will be incorporated into the safety case, and that simulated inputs from other divisions would include delays to allow correct operation to be confirmed. The RP subsequently included these responses in an updated report (Ref. 234).

461. The submission 'Strategy for Conducting ICBMs Activities for RPS [PS]' (Ref. 211) described how the CIM-1 (the 'original' CIM design from the reference plant) will be HPD-based, and that the HPD ICBM techniques such as formal equivalence checking will be applied to this. However, it stated that there are a small number of inputs to the CIM and that these are well defined, and that if the CIM internal state space is non-complex then it may be possible to perform exhaustive testing of this design. The submission stated that further consideration of this will be performed after the CIM-1 detailed design is completed during site-specific stages of the project.

462. I observe that exhaustive testing, in conjunction with suitable engineering analyses and qualification, can provide very high confidence that low complexity systems will perform correctly under all operational conditions. The confidence provided by exhaustive testing is such that I consider it appropriate that all reasonably practicable efforts should be made to design the CIM-1 so that it can be exhaustively tested and so it can be demonstrated that all hazards associated with the design can be adequately managed. The importance of this observation is such that I raise this as an Assessment Finding:

AF-UKHPR1000-0043 – The licensee shall demonstrate that the programmable hardware-based Component Interface Module can be exhaustively tested and that all risks associated with the design are reduced so far as is reasonably practicable.

4.7.1.2 SAS ICBM Strategy

463. The submission 'Strategy for Conducting ICBMs Activities for SAS' (Ref. 222) provides information on ICBMs specific to the SAS. The SAS is based on the same FirmSys platform as the RPS [PS] and for this reason the ICBMs are similar and are as reflected in the common sections of each ICBM strategy document, and previously described in paragraphs 449 and 450. Differences reflect the fact that the highest categorisation of safety functions performed by the SAS are Category B. So, for example, the PE review activities apply IEC 62138 (Ref. 22), and IEC 62566 part 2 (Ref. 25), as these are suitable for Category B and C safety functions. It is stated that statistical testing is difficult to apply to the SAS as this mainly provides control and display of plant equipment, and there is no defined operational profile. This point is accepted for GDA, but I note that ST would not be applied until the SAS design is

complete and further research in the interim may identify that ST is beneficial and is reasonably practicable in this case. My expectation is that this research will be revisited by the licensee as part of normal business at the detailed design stage of the project.

464. The lower-classification of the SAS means that source code comparison was not considered reasonably practicable at the time of GDA. However, I note that it is recognised that developments in tools and greater automation may mean that this becomes reasonably practicable at the time of deployment.

4.7.1.3 PSAS and KIC [PCICS] ICBM Strategy

465. The submission 'Strategy for Conducting ICBMs Activities for PSAS and KIC [PCICS]' (Ref. 230) states that both PSAS and KIC [PCICS] are F-SC3 classification systems based on the HOLLiAS-N platform. The submission further states that the design of both these systems are based on the reference design but are not complete during GDA. However, an outline description of each system design is provided, giving information on the application software development process, including software tools. Independent review of PE activities includes reviews of development processes against relevant standards, the quality plan, the software validation plan, type testing, and operational experience (claimed to be based on significant previous deployment). The main ICBMs identified for these two systems include the PE reviews described above and independent commissioning tests. It is stated that some components of the PSAS and KIC [PCICS] systems contain third party software, and it is unlikely that design information on these will be available for ICBMs to be applied to them. It is stated that further consideration of ICBMs, and a strategy for their application will be the responsibility of the licensee. Noting the design of these systems is not complete, I consider the proposed ICBMs are reasonable for the purposes of GDA. However, I observe that particularly where third party software is used, a demonstration of adequate risk control will need to be made during site-specific stages of the project. For this reason, I raise the following Assessment Finding:

AF-UKHPR1000-0044 – The licensee shall, for all systems which contain third party software, develop a strategy for independent confidence building measures which, together with appropriate production excellence, allows risk control to be demonstrated.

4.7.1.4 KDA [SA I&C] ICBM Strategy

466. The 'Strategy for Conducting ICBMs Activities for KDA [SA I&C]' (Ref. 231) states that the KDA [SA I&C] is a F-SC3 (Class 3) system based on the SpeedyHold platform. The submission further states that the design of this system is based on the reference design, but is not complete during GDA. However, an outline description of the system design is provided, giving information on the application software development process, including software tools. Independent review of PE activities includes reviews of development processes against relevant standards, the quality plan, the software validation plan, type testing, and operational experience (claimed to be based on previous deployment). The main ICBMs identified for this system include the PE reviews described above and independent commissioning tests. It is stated that some components of the KDA [SA I&C] system contains third party software, and it is unlikely that design information on these will be available for ICBMs to be applied to them. It is stated that further consideration of ICBMs, and a strategy for their application will be the responsibility of the licensee. Noting the design of this system is not complete, I consider the proposed ICBMs are reasonable for the purposes of GDA. However, I note that the application of further ICBMs may become reasonably practicable as the design is established during site-specific stages of the project. I have raised AF-UKHPR1000-0044 to provide assurance that appropriate ICBMs will be identified for systems containing third party software.

4.7.2 Strengths

467. The approach to the application of ICBMs is aligned with modern international standards and UK RGP. It is graded according to system classification and recognises that further research and development of ICBMs will be necessary to determine the full extent of the ICBMs that will be reasonably practicable at the time that the UK HPR1000 systems will need to be fully substantiated. This is good practice.

4.7.3 Outcomes

468. My assessment of the submissions relating to ICBMs (Ref. 211), (Ref. 222), (Ref. 230) (Ref. 231) identified an acceptable approach to the identification and application of ICBMs that is appropriately graded according to system classification and that is diverse from the system PE. Similarly, I was content with the approach to ST, as set out in (Ref. 234). I was content with this approach, and closed RO-UKHPR1000-0057 (Ref. 40), with a closure note (Ref. 228).

469. I identified two AFs in the area of ICBMs, AF-UKHPR1000-0043 relating to design decisions for the CIM-1 to achieve exhaustive testing, and AF-UKHPR1000-0044 relating to ICBMs for systems containing third party software.

4.7.4 Conclusion

470. I am satisfied with the ICBM methodology that has been set out in the ICBM submissions (Ref. 211), (Ref. 222), (Ref. 230) (Ref. 231) during GDA Step 4. In my opinion this meets the requirements of the relevant international standards and UK RGP, and satisfies SAP ESS.27 and NS-TAST-GD-046. I judge the approach to ST, as set out in (Ref. 234) to be acceptable for the purposes of GDA.

4.8 Cyber Security of C&I Systems

4.8.1 Assessment

471. I worked closely with the ONR CS&IA inspector to assess the demonstration of cyber security of C&I systems important to safety. The key SAP (Ref. 2) considered in my assessment was ESS.27, and in particular the guidance provided in appendix 6 of NS-TAST-GD-046 (Ref. 10). My assessment has also been informed by the relevant SyAPs (Ref. 5) – in particular FSyP 7 and the related detailed principles SyDP 7.1 – SyDP7.5. I have also considered RGP for cyber security, in the form of the national cyber security centre's (NCSC) secure design principles (Ref. 236) and commercial product assurance (CPA) build standard (Ref. 237), and international standards including IEC 62645 (Ref. 26) and IEC 62859 (Ref. 27).

472. ONR's judgement against the expectations of the SyAPs (Ref. 5) is documented in the security assessment report (Ref. 238). The CS&IA assessment against the expectations of FSyp7 is detailed in an assessment note (Ref. 7). I have not made a judgement against the SyAPs in this report, although my assessment has been informed by the conclusions reached by the CS&IA inspector.

473. The C&I TSC also provided support to this assessment (Ref. 36). I have considered both the ONR TSC's findings and those of the ONR CS&IA inspector as part of my assessment.

474. During GDA Step 3 (Ref. 128) I reviewed the RP's 'Cyber Security Risk Assessment Methodology' (Ref. 239) and raised RQ-UKHPR1000-0364 (Ref. 109) seeking clarification on the scope of the risk assessment. To address this, in GDA Step 4 the RP provided a revised methodology (Ref. 240). My review of this submission found that my queries had been addressed, and also that the methodology had been supplemented with further information to demonstrate how the requirements of key

standards, including IEC 62645 (Ref. 26) and IEC 62859 (Ref. 27), had been addressed. I was content that the methodology presented a suitable approach to cyber security risk assessment and that it had appropriately considered RGP.

475. In GDA Step 4 the RP provided a 'Cyber Security Risk Assessment Report' (CSRAR) (Ref. 241) documenting the application of the cyber security risk assessment methodology to the centralised C&I systems. Detailed assessment of this was led by the CS&IA inspector (Ref. 7) with my support and is not repeated here. The relevant findings from my assessment are summarised in the following paragraphs.

476. My review of the CSRAR (Ref. 241) and identified a number of queries regarding the outcomes of the risk assessment. Of particular significance were the following:

- The assessment had not considered the KDS [DAS] as this is based on simple hardware technology which is invulnerable to cyber-attack. Whilst I was content that the safety functions of the KDS [DAS] are delivered by hardware technology, I was concerned that the risk assessment had not considered whether a cyber-attack targeting the programmable elements of the system (i.e. the monitoring and test cards) could propagate to other systems and compromise the delivery of safety functions.

- The HMI of the KDA [SA I&C] system runs on an obsolete operating system, which is no longer supported by the vendor . The RP claimed that the system supplier would "…patch/ work around any new identified [operating system] vulnerabilities" but did not provide any justification that this was a credible and appropriate course of action.

477. To address these concerns, I raised RQ-UKHPR1000-1172 (Ref. 109). In response the RP provided a detailed description of how the programmable elements of the KDS [DAS] were considered in the cyber risk assessment and how there was adequate protection against propagation from a cyber-attack. I was content with this explanation.

478. The RP also made a commitment to modify the KDA [SA I&C] to use an up-to-date operating system, although this modification has not been implemented within GDA. The RP has implemented a further modification to the design of the KDA [SA I&C] (Ref. 200), discussed further in Section 4.5.3 of this report, which reduced reliance on the computer-based HMI for operation of the system. Nevertheless, I consider it important to ensure that the modification to upgrade the operating system is correctly implemented to reduce vulnerability to cyber-attack. I have therefore raised this as part of Assessment Finding AF-UKHPR1000-0046 below.

479. The RP provided a revised submission of the CSRAR (Ref. 242), incorporating the response to RQ-UKHPR1000-1172 (Ref. 109). I reviewed this and was content that my concerns had been satisfactorily addressed. I also found that the security degrees assigned to each system had been informed by its safety Class. From a C&I perspective I judge that the system security degrees are appropriate, with the systems of highest safety significance being assigned to the most onerous security degree.

480. The CSRAR (Ref. 242) documents the risk assessment of the centralised C&I systems but states that the non-centralised C&I systems have not been risk assessed due to being out of scope for GDA. While I acknowledge that this is aligned with defined the scope of GDA (Ref. 243) I consider it important to ensure that the non-centralised systems are subjected to a risk assessment using an appropriate methodology. However, the input to this risk assessment will be impacted by licensee design choices and detailed design information and hence I have raised an Assessment Finding for this to be addressed by the licensee.

AF-UKHPR1000-0045 – The licensee shall, as part of detailed design of the C&I systems, develop the cyber security risk assessment to include all C&I systems important to safety, and all interfaces between and within those systems. The assessment should follow a methodology that is at least as rigorous as that developed for GDA, and should include demonstration that measures are in place to address all identified vulnerabilities.

481. My review of the CSRAR (Ref. 242) found that it identified a number of vulnerabilities; these were all related to interfaces to systems that were outside the scope of assessment during GDA. The CSRAR specifies a requirement for these vulnerabilities to be addressed through design modifications to be implemented post-GDA. While I acknowledge that the implementation of these modifications will depend on licensee design choices and detailed design information, I consider it important that ONR tracks them to completion. I have therefore raised an Assessment Finding for this to be addressed by the licensee.

AF-UKHPR1000-0046 – The licensee shall resolve the residual cyber security vulnerabilities identified in the GDA cyber security risk assessment report as part of detailed design. This should include the potential modifications proposed during GDA.

482. A key regulatory expectation for GDA is that requirements for C&I systems are clearly specified, and I therefore sought an understanding of how the outcomes of the cyber security risk assessment would be integrated into the C&I design process. The RP produced a 'Cyber Security Design Requirements Specification' (CSDRS) (Ref. 244) to translate the control sets identified in the CSRAR (Ref. 242) into a set of technical requirements to be implemented in the design of the systems.

483. I reviewed the CSDRS and identified a number of areas where there was a lack of clarity in the specified requirements that could lead to incorrect interpretation and implementation. I therefore raised RQ-UKHPR1000-1434 (Ref. 109) to seek further clarification. The RP's response explained how the CSDRS would be updated to remove ambiguity and provide greater clarity on how the control sets should be implemented. The RP subsequently submitted a revised CSDRS (Ref. 245) which I reviewed and was content that my concerns had been addressed.

484. I sampled the SRS (Ref. 151) and SDS (Ref. 212) for the RPS [PS], to understand how cyber security has been considered in the system design process. I found that the SRS provided high-level requirements for cyber security and provided a reference to the CSDRS for specific requirements on how the control sets should be implemented. I further found that the SDS elaborated the requirements, albeit still at a high-level, and provided references back to the parent requirements in the SRS. Further discussion of the management of requirements through system design is provided in sub-sections 4.6.1 – 427 of this report, but for the cyber security assessment I was content from a C&I perspective that the outcomes of the cyber security risk assessments had been integrated into the C&I system design process.

485. The RP undertook analysis of the RPS [PS] and PSAS to determine the extent to which the current design of the C&I systems aligns with the cyber security requirements identified in the CSDRS (Ref. 245), and submitted the results to ONR (Ref. 246) and (Ref. 247). I reviewed these submissions and identified several concerns, most notably the following:

- There were several instances where the analyses showed non-compliance with requirements that were stated as being 'mandatory'. The justification of acceptability of these gaps was inadequate and made assumptions that suitable compensation will be implemented by the licensee.

- Commitments and forward action plans did not give confidence that the outcomes of the cyber security risk assessment will be completely and correctly implemented in the C&I design.

486. I therefore raised RQ-UKHPR1000-1705 (Ref. 109) asking the RP to provide further explanation of the gaps identified and the actions that will be required of the licensee to address these gaps. In response to this the RP submitted revised versions of the compliance analyses (Ref. 248) and (Ref. 249). My review found that the RP had identified all instances of partial and non-compliance, that appropriate compensating measures to bring about compliance had been specified, and that clear commitments for the licensee to implement these measures were made.

487. While the analyses undertaken within GDA give some confidence that cyber security will be adequately implemented in the C&I system designs, I consider it important to ensure that the identified non-compliances with cyber security requirements are completely and correctly resolved as the design progresses. It is also important to ensure that the cyber security compliance analysis process is completed for all C&I systems. These activities will be dependent on detailed design information and will be subject to licensee design choices, and on this basis I have raised an Assessment Finding for the licensee to address this.

AF-UKHPR1000-0047 – The licensee shall complete cyber security compliance analysis for all computer-based C&I systems important to safety and shall implement measures to address all instances of partial or non-compliance.

488. An important regulatory expectation for the design of computer-based systems is the demonstration of how cyber security is taken into account in the design of platforms and systems. This has similarities with the expectations for production excellence, as described by SAP ESS.27. The detailed assessment of the PE of C&I platforms and systems is documented in sub-sections 195 – 427 of this report. The following paragraphs describe the aspects of PE relevant to cyber security.

489. My review of the CSRAR (Ref. 242) found that it discusses PE for cyber security and refers out to PE justification documents for the C&I platforms and systems. It also recognises that the standards against which PE is judged from a safety perspective may not give sufficient consideration to security and therefore provides a compliance analysis against the NCSC CPA build standard (Ref. 237). While no non-compliances are identified, the analysis does identify actions for the licensee to undertake in order to ensure full compliance. These are captured as requirements to be implemented by the licensee.

490. The RP also makes compliance statements against the NCSC secure design principles (Ref. 236). This is a welcome approach and whilst many of the compliance statements are high-level, I consider it a positive that the RP has considered this aspect of RGP.

491. As part of the resolution of RO-UKHPR1000-0059 (Ref. 40) the RP identified several gaps in the PE of the FirmSys platform. This included a gap related to the definition of security design principles. The FirmSys production excellence assessment (Ref. 72) describes the gap as follows: “The assessment identified that the FirmSys platform incorporates a number of security design features such as access management and security maintenance network design indicating there is a level of security awareness for the design. However, there are no documented overarching plans or design guidelines which set out the security aims for the platform to inform the selection of appropriate security design features. As a result, no justification exists to demonstrate that there is no capability for unauthorised access via data links to the protection system.”

492. To address this gap the RP identified, in the document 'Assessment Report of Production Excellence for FirmSys Platform' (Ref. 72), a series of compensating measures, including undertaking further security risk assessment of FirmSys from which a complete set of security requirements will be captured and taken through to implementation. The RP also provided a justification as to the suitability of these measures and has defined a forward action plan for how they will be implemented. While I was in agreement with the RP's findings I consider it important that this work is tracked to completion in order to ensure the FirmSys platform can be demonstrated to by adequately protected against a cyber-attack. My expectation is that this will be addressed as part of Assessment Finding AF-UKHPR1000-0031 (see sub-section 195).

493. Another regulatory expectation is that the licensee will provide a rigorous demonstration that measures to achieve cyber resilience do not adversely impact upon the safety performance of C&I equipment and systems, and that this demonstration will include independent assurance to provide additional confidence. While these activities will typically be carried out during site-specific stages, an important aspect of my assessment was seeking confidence in the strategy for cyber security assurance. My review of the CSRAR (Ref. 242) found that, while some information relating to independent security assurance measures (ISAM) was provided, there was insufficient information to gain confidence in the strategy. In particular I noted the following:

- No details were provided on specific activities to be carried out, for example requirements, methodologies and success criteria.
- A number of activities appeared not to be independent from system development.
- No justification was provided as to the suitability of the proposed activities.
- It was unclear which activities would apply to which systems.
- There was no clear commitment for the licensee to undertake the independent assurance activities.

494. I therefore raised RQ-UKHPR1000-1584 (Ref. 109) requesting the RP to define the strategy for undertaking ISAM during site-specific stages. The response to this RQ outlined a methodology which was graded based on the safety and security significance of systems, and described a range of assurance activities that will be implemented. While this gave some confidence in the ISAM strategy, there remained a lack of clarity over specifically which activities would be applicable to each system.

495. I therefore raised RQ-UKHPR1000-1707 (Ref. 109) asking the RP to provide the complete strategy for ISAM that will be implemented by the licensee. The response to this RQ provided a comprehensive set of tables that described each activity in detail, including methods, independence measures and success criteria, and clearly showed which activities would apply to which systems. I judged this response to be adequate and was satisfied that the RP has provided sufficient confidence in the strategy for independent cyber security assurance. However, given the significance of the programme of work I consider it important that ONR tracks this issue to resolution. I have therefore raised an Assessment Finding for this to be addressed by the licensee.

AF-UKHPR1000-0048 – The licensee shall implement independent security assurance measures for the UK HPR1000 C&I systems important to safety. These should address, as a minimum, the following:

- measures to provide confidence that adequate security arrangements have been put in place by equipment suppliers to minimise security risks impacting C&I system development;
- measures to provide confidence that security design risks impacting the safety performance of C&I systems are adequately mitigated;

- a graded approach to the levels of rigour and independence required for assurance measures that is informed by the safety and security significance of the system or equipment;
- assurance that security has been considered throughout the development lifecycle of systems;
- definition of the activities to be undertaken including objectives, inputs, outputs, methods and success criteria; and
- the organisational capability and capacity required to undertake independent assurance activities.

The independent security assurance programme should be in accordance with the strategy submitted in GDA, or an equivalent alternative.

4.8.2 Strengths

496. The RP has developed a methodology for cyber security risk assessment that is aligned with RGP and has applied this methodology to the centralised C&I systems. The outcomes of the cyber security risk assessment have been translated into a set of high-level design requirements that have been integrated into the C&I design process.

497. The RP has developed a comprehensive strategy for undertaking independent assurance of cyber security.

4.8.3 Outcomes

498. The outcome of my assessment of cyber security of C&I systems important to safety identified four residual matters that have not been resolved within GDA timescales; these are summarised below:

- The cyber security risk assessment of the non-centralised C&I systems has yet to be completed.
- Several design modifications to address cyber security vulnerabilities have not been implemented in GDA.
- The cyber security compliance analysis has yet to be completed for all C&I systems.
- The strategy for independent cyber assurance should be implemented by the licensee.

499. These matters have been taken forward as Assessment Findings.

4.8.4 Conclusion

500. On the basis of the evidence sampled in my assessment of cyber security for C&I systems I have concluded that the cyber security risk assessment adequately demonstrates that cyber security risks are adequately protected by the controls identified by the RP, and that cyber security is effectively integrated into the C&I design process. From a C&I perspective I am satisfied that the risk of a cyber-attack compromising safe operations is adequately controlled and that the expectations described in Appendix 6 of NS-TAST-GD-046 (Ref. 10) have been adequately met in the context of GDA. The CS&IA inspector concluded (Ref. 7) that “the case presented within the Generic Security Report (GSR) is adequate” and that the expectations of SyAP (Ref. 5) FSyp7 have been met; this has informed my judgement.

4.9 Adequacy of Human-machine Interfaces

4.9.1 Assessment

501. A Human-machine Interface (HMI) is a device that allows an operator to interact with C&I systems. They are required for manual control of plant, plant monitoring, and plant

operating mode changes. On the UK HPR1000 each of the centralised C&I systems has an associated HMI system. The HMI systems are a part of the centralised C&I system with which they interact, therefore are expected to inherit appropriate requirements from their parent systems, including classification. An HMI can either be computerised or hardwired. Hardwired in this document refers to an HMI which rely on analogue devices to communicate directly with software based systems and analogue devices interfacing directly with non-computerised systems.

502. In my assessment of the adequacy of HMI I have considered the following key areas:

- Category of functions supported by HMI systems.
- Classification of HMI systems.
- Suitability of HMI safety requirements.
- Suitability of HMI technology choices.
- Alarms.
- Adequacy of HMI Safety Case.

503. The key SAPs that were considered in this aspect of my assessment included:

- SC.4 Safety case characteristics;
- ECS.1 Categorisation of safety functions;
- ECS.2 Classification of structures, systems and components;
- EDR.2 Redundancy, diversity and segregation;
- EDR.3 Common cause failure;
- ESS.2 Safety system specification;
- ESS.17 Faults originating from safety systems;
- ESS.20 Avoidance of connections to other systems;
- ESS.21 Reliability;
- ESS.22 Avoidance of spurious actuation;
- ESS.27 Computer based safety systems;
- ESR.1 Provision in control rooms and other locations; and
- EHF.7 User interfaces.

504. The high-level architecture for the HMI of the UK HPR1000 is detailed in Chapter 8 of the PCSR (Ref. 107) and described in greater detail in ‘Strategy for the use of HMIs’ (Ref. 250) The HMI architecture comprises the following panels:

- Operator Workplace (OWP).
- Emergency Control Panel (ECP).
- Protection System Panel (PSP).
- Auxiliary Control Panel (ACP).
- Large Display Panels (LDP).
- Diverse Human-interface Panel (DHP).
- Severe Accident Human-interface Panel (SHP).
- Compact Operator Workplaces (COWP).
- Hard Control Panel (HCP).

505. These panels each employ a variety of HMI devices. Across the panels, these devices are:

- Protection System Safety Control and Information Device (PS-SCID200).
- Safety Automation System Safety Control and Information Device (SAS-SCID200).
- SAS-SCID300.
- Plant Computer Information and Control System KIC [PCICS] – Visual Display Unit (KIC-VDU [PCICS]).
- Auxiliary Control Panel – Visual Display Unit (ACP-VDU).
- Severe Accident Human-interface Panel – Visual Display Unit (SHP-VDU).

- Various hardwired equipment.

506. Each panel incorporates multiple types of HMI, and often multiple instances of a single type.

507. The panels and HMI devices detailed above are used throughout the Main Control Room (MCR), Remote Shutdown Station (RSS), and Technical Support Centre. I focussed my assessment on the MCR and RSS as these are the rooms where the majority of HMI associated with the centralised C&I systems are located. Table 3 describes the main UK HPR1000 HMI devices, the panels in which they are used and their safety classifications.

Table 3: Designation of UK HPR1000 HMI devices

HMI	Panels	Safety Class
KIC-VDU(Note 1)	OWPs COWPs LDP	F-SC3 (Cass 3) / Non-Classified (NC)
SAS-SCID200	OWPs COWPs	F-SC2 (Class 2)
SAS-SCID300	ACPs HCP	F-SC2 (Class 2)
PS-SCID200	ECP PSP HCP	F-SC1 (Class 1)
ACP-VDU	ACPs	F-SC3 (Class 3)
ACP-VDU	LDP	NC
Hardwired Equipment(Note 2)	ECP ACPs HCP SHP DHP	F-SC1 (Class 1) / F-SC2 (Class 2) / F-SC3 (Class 3)
SHP-VDU	SHP	F-SC3 (Class 3)
Reactor Trip Buttons	HCP	F-SC1 (Class 1)

HMI	Panels	Safety Class
MCR/RSS Mode Switches	HCP RSS Switch Boxes	F-SC1 (Class 1)

Note 1 – the KIC-VDU is classified as Class 3 as its use in the OWP is to perform Category C safety functions. However, it is also deployed in the non-classified LDP.
Note 2 – there is a large variety of hardwired HMI equipment deployed in various panels at different classifications.

508. The Technical Support Centre also contains a COWP. This is only used when operators require support from the technical support staff. This has not been considered in my assessment as I focussed on areas of a greatest safety significance.

509. During GDA Step 3 the RP submitted 'Overall Scheme for Control Room System' (Ref. 251). This document provided a detailed explanation of the layout of the workstations in both the MCR and RSS. I have not considered the detailed information relating to the layout of the MCR and RSS during GDA; this is because the detailed human factors requirements have yet to be developed for the UK HPR1000 and these may necessitate modification to the layout. I consider this to be a part of normal business during site-specific stages.

510. Having reviewed 'Overall Scheme for Control Room System' (Ref. 251) I raised RQs RQ-UKHPR1000-0321 and RQ-UKHPR1000-0354 (Ref. 109), in relation to the proposed use of touchscreen technology in the PS-SCID200. I raised the use of touchscreen technology in a Class 1 system as an issue in my Step 3 assessment note (Ref. 128). During GDA Step 4, I raised a further RQ, RQ-UKHPR1000-0817 (Ref. 109) to gain a greater understanding of the RP's justification for the use of touchscreen.

511. I also raised RQ-UKHPR1000-0812 during GDA Step 4, raising wider concerns regarding the interconnections found between C&I systems. With specific regard to HMIs I noted that there was an interconnection between the Class 3 KIC-VDU [PCICS] and Class 2 SAS-SCID200 which had not been adequately justified.

512. I assessed the RQ responses and I was unable to make a judgement as the information available was not sufficient. There were no safety functional requirements detailing what the HMIs needed to achieve nor was there any clear justification for the touchscreen technology nor was there any indication in the BSC documents that the HMI was considered within the safety case. I therefore raised RO-UKHPR1000-0052 'Design and Safety Case for Class 1 and 2 Human Machine Interfaces Employed in the Main Control Room and Remote Shutdown Station' (Ref. 40) to:

- Understand the safety functional and performance requirements for the Class 1 and Class 2 HMI in the MCR and RSS.
- Ensure the RP performs and presents an adequate optioneering study for the Class 1 and Class 2 touchscreen HMI.
- Ensure that a suitable and sufficient Safety Case for Class 1 and Class 2 HMI in the MCR and RSS was presented during GDA.

513. My detailed assessment of the response to this RO is documented in an assessment note (Ref. 252) and is not repeated in full here. However, the key points are summarised throughout the HMI assessment. As the RO fundamentally dealt with every aspect of the HMI safety case, for clarity the three actions are referenced throughout this section of the report.

4.9.1.1 HMI Categorisation and Classification

514. PCSR Chapter 8 (Ref. 107) and the BSCs of the centralised C&I systems (Ref. 99) – (Ref. 102) describe the classification of the HMI systems. The design specifications of the centralised C&I systems (Ref. 212) – (Ref. 253) describe the safety category of the functions performed by the C&I and supported by the HMI. The design specifications also describe the targeted reliability as a pfd. The HMI does not perform its assigned functions alone but rather supports those functions. Table 4 details the key information from these documents for the purposes of this section.

Table 4: Classification and reliability targets of UK HPR1000 HMI equipment

Centralised C&I System	Category of Functions Performed	C&I System Classification / Targeted pfd	Primary HMI Device	Category of Functions Supported	HMI System Classification / Targeted pfd
Protection System	Category A	Class 1 / 10^{-4}	PS-SCID (200)	FC2 (Category B)	F-SC1 (Class 1) / 10^{-3}
Safety Automation System	Category B	Class 2 / 10^{-3}	SAS-SCID (made up of both SAS-SCID200 and SAS-SCID300)	FC2 (Category B)	F-SC2 (Class 2) / 10^{-3}
Plant Standard Automation System	Category C	Class 3 / 10^{-1}	KIC – VDU [PCICS]	FC3 (Category C)	F-SC3 (Class 3) / 10^{-1}
Diverse Actuation System	Category B	Class 2 / 10^{-3}	DHP	FC2 (Category B)	F-SC2 (Class 2) / 10^{-3}
Severe Accident System	Category C	Class 3 / 10^{-1}	KDA [SA I&C] HMI	FC3 (Category C)	F-SC3 (Class 3) / 10^{-1}

515. A key expectation in my assessment of the classification of the HMI is that they align with the classification of the system that the HMI supports, are sufficient for the category of function that the HMI supports, and that the reliability targets are appropriate for the safety significance of the system that the HMI supports. I found in my assessment that the assessed HMI systems have been assigned an appropriate classification with the systems with which they interface and the functions that they perform. I was satisfied that the relevant expectations of SAPs ECS.1 and ECS.2 have been met. I did note a discrepancy between the reliability target for the PS-SCID and that for the RPS [PS] (see sub-section 4.3.1); this is discussed further in sub-section 4.9.1.5.

4.9.1.2 Suitability of HMI safety requirements

516. Action 1 of RO-UKHPR1000-0052 (Ref. 40) required the RP to provide the safety and performance requirements for Class 1 and Class 2 HMI in the MCR and RSS. This includes both computerised and hardwired HMI and therefore include the HMI for the RPS [PS], SAS, and KDS [DAS]. I have not considered the Class 3 or non-classified

safety requirements for systems as my assessment has focused on those systems with the highest safety significance.

517. I assessed the documentation detailing the safety functional and performance requirements for Class 1, Class 2, and hardwired HMI (Ref. 254) (Ref. 255) (Ref. 256). These were submitted for action 1. I found in my assessment that these, in general, presented clear traceability from a source through to a requirement. However, often the rationale cannot be found as to why certain requirements have been chosen or why these are adequate. The adequacy of requirements is discussed further in sub-section 4.6.1 and has been taken forward by Assessment Finding AF-UKHPR1000-0034 (see sub-section 4.6.1).

518. I assessed the documentation detailing the design specification for the Class 1, Class 2, and hardwired HMI (Ref. 212) (Ref. 219) (Ref. 257). These were submitted for action 1. I found in my assessment that the incorporation of the HMI specification into the design specification of the relevant systems (i.e. the PS-SCID into the RPS [PS] design specification) integrated the HMI into the wider safety case compared with prior to RO-UKHPR1000-0052 (Ref. 40). In general, I found that these design specifications linked with the requirement specifications well, with clear traceability employed by using unique identifiers. However, I did note that the design specification read as a paraphrase of the requirements specification. I expect that design specifications should be more detailed than these with a clear description of how the requirements will be met. I note that the specification of detailed design requirements will depend on human factors requirements, which have not been specified within GDA. I judge this lack of detail in the design specifications to be a minor shortfall that should be addressed by the licensee as part of detailed design and substantiation of the HMI equipment. On the basis of the evidence sampled I was content that the RP had adequately addressed action 1 of RO-UKHPR1000-0052 and hence the action was closed.

4.9.1.3 Suitability of HMI technology

519. A key aspect of my assessment was establishing confidence in the suitability of the technology on which the HMI are based. I focussed my assessment on the Class 1 and Class 2 HMI in the MCR and RSS as my assessment has focused on those systems with the highest safety significance.

520. For action 2 of RO-UKHPR1000-0052 I assessed the RP's optioneering reports for Class 1 computerised HMI and Class 2 computerised HMI (Ref. 258) (Ref. 259). These detailed the optioneering studies performed for the HMI which analysed touchscreen and various other technologies. I was satisfied in my assessment of these reports that the intent of action 2 had been met and that an appropriate range of technologies was considered (Ref. 252).

521. I noted however that the optioneering studies had not adequately considered the hazards (such as the consequences of internal failures) of the analysed technologies. No form of hazards analysis was included in the description of the technologies. Due to the implementation of sensitivity analysis following the ranking of the options, in the case of these reports, I was of the opinion that the risk was adequately mitigated. I judge the failure to consider the hazards associated with the analysed technologies, such as those caused by internal faults and failures, in the optioneering studies to be a minor shortfall against the expectations of SAPs SC.4 and EDR.1 that will be dealt with as part of normal business during site specific stages.

522. The optioneering studies (Ref. 258) (Ref. 259) presented the PS-SCID200 and SAS-SCID200 selected options as a keyboard and mouse combination and the SAS-SCID300 as a tracker ball. I consider these options to be appropriate for their classification requirements and that they align with the control room designs of other nuclear installations in the UK.

523. The hardwired HMI technology is described in 'Class 1 and 2 Hardwired HMI Design Specification' (Ref. 260) and 'Analysis Report for Class 1 and 2 Hardwired HMI' (Ref. 261). This details the RP's intended approach to hardwired HMI including the use of push buttons, switches, lamps, and indicators. Hardwired HMI technology is employed by the RPS [PS] for those Category A manual functions that the PS-SCID200 is not assigned to along with a number of key alarms and the DHP. I consider the technology choices to be appropriate for their intended functions.

524. I consider that it is important for overall HMI technology choices to ensure that diversity is maintained across all C&I systems and the that use of HMI does not compromise the safety principles employed by the C&I systems they support, such as CCF and redundancy. My assessment considered this and found that diversity is ensured across the UK HPR1000 control room by using differing HMI technologies for the centralised C&I systems. The RPS [PS] and SAS both use versions of the SCID for their computer-based HMI. The SCID is based on the FirmSys platform which is common to both systems. I judge this to be acceptable, because both the RPS [PS] and SAS belong to the same layer of defence in depth (as described in Section 4.3), and both systems also incorporate hardwired HMI technology.

525. The RP is developing a hardware-based platform KDS [DAS] or diverse actuation system as the secondary line of protection and this is designed to use hardwired HMI on the DHP as discussed above. I consider that this selection of HMI technologies maintains the diversity of the C&I systems and adequately reduces the risk of Common Cause Failure caused by HMI. The redundancy requirements of the HMI systems are inherited from their parent systems. I judge that the HMI in the MCR and RSS meets the requirements of SAPs EDR.2 and EDR.3.

526. On the basis of the evidence sampled I am content that the RP's approach to HMI technology selection is suitable for the claims on the HMI systems.

4.9.1.4 Alarms

527. The document 'Alarm Function and Alarm Processing Requirement Specification' (Ref. 262) details the generic requirements for alarms and alarm processing in the UK HPR1000. The 'Class 1 and Class 2 Hardwired HMI Requirements Specification' (Ref. 256) describes the requirements for hardwired alarms.

528. During GDA Step 3 I raised RQ-UKHPR1000-0289 (Ref. 109) to understand the inclusion of Category A alarm functions and indications. The RP's response explained that the UKHPR1000 does not include Category A alarms, but it does include Category A indications. The response explained that the alarms and indications would be displayed on the Class 3 KIC-VDU [PCICS].

529. My assessment of the 'Class 1 and Class 2 Hardwired HMI Requirements Specification' (Ref. 256) found that there was still a lack of clarity as to the means of displaying these Category A indications. I therefore raised RQ-UKHPR1000-1651 (Ref. 109) during GDA Step 4 to confirm that these indications and alarms would also be displayed on hardwired Class 1 and Class 2 HMI.

530. The response to this RQ confirmed the following:

- all Category A indications will be displayed via Class 1 Hardwired HMI;
- all Category B indications will be displayed via Class 2 SAS-SCID300;
- all Category B alarms will be displayed via Class 2 Hardwired HMI on the ACP panel; and
- the KIC [PCICS] system provides monitoring and alarm functions under all conditions of the plant where it is operational.

531. The specific functions that will be alarmed are identified in the 'Class 1 and Class 2 Hardwired HMI Requirements Specification' (Ref. 256) as to be decided during site-specific stages. This is reasonable for GDA, as the design is not yet detailed enough to present the finalised alarm arrangements.

532. I judge the provision for alarms at this stage in the design to be adequate for the purposes of GDA, though I expect further design to take place during site-specific stages where specific human factors requirements will be developed via suitable analysis for the alarms.

4.9.1.5 Adequacy of HMI Safety Case

533. Action 3 of RO-UKHPR1000-0052 (Ref. 40) required the RP to present a suitable and sufficient safety case for the HMI. For my assessment of this action, I sought confidence that a suitable and sufficient safety case had been provided and that it addressed the specific shortfalls identified in the RO. In general, I found that the shortfalls had been addressed. However, I also identified a number of residual matters which I describe in the below paragraphs.

534. The computer-based HMI for Class 1 is provided by the PS-SCID; this is used to control permissive functions, operating bypass, and safety function reset, among other controls. The functional categorisation of the functions the PS-SCID supports is Category B. Typically a system supporting Category B functions would be Class 2, however the documents explain that the PS-SCID is F-SC1 (Class 1) to reduce the likelihood of a malfunction impacting the Class 1 RPS [PS]. I consider this to be a reasonable philosophy for managing the risk of interference of lower-class equipment on higher-class systems. However, the reliability of the PS-SCID is defined as 10^{-3} pfd in comparison to the higher reliability of the protection system of 10^{-4} pfd. The functions associated with the PS-SCID have a required pfd of 10^{-3}. I was concerned about this mismatch, and in particular the potential for the less-reliable HMI to inject errors into the RPS [PS]. I raised RQ-UKHPR1000-1578 (Ref. 109) to query this, specifically querying the consequences of spurious actuation of the permissive functions or failure on demand of the permissive functions.

535. The response to RQ-UKHPR1000-1578 (Ref. 109) stated that the spurious actuation of the permissive signals is prevented by linking the manual signal with an automatic signal within the PS, this automatic signal is a Category A function. The failure on demand of the permissive signal could be detected by the KIC [PCICS], but the design does not provide mitigation of the fault. The operator would be required to hold the plant in its current state and await repair of the PS-SCID. No justification was provided as to why this would be acceptable.

536. My assessment of RQ-UKHPR1000-1578 (Ref. 109) concluded that the RP has not sufficiently justified the categorisation of the permissive signals, given their potential to fail and prevent plant operations from correctly proceeding. This is a particular concern given the number of permissive signals present in the design. I judge this to be a shortfall against the expectations of SAP ECS.1. However, resolution of this shortfall will require detailed design information and on this basis I have raised an Assessment Finding for the licensee to carry out a review of the permissive functions for the UK HPR1000 C&I.

AF-UKHPR1000-0049 – The licensee justify the permissive safety functions on UK HPR1000 C&I systems important to safety. The justification shall consider all permissive signals and should as a minimum address the following:

- the potential consequences of the failure of the Protection System -Safety Control and Instrumentation Device to act when required in all operating modes;

- the potential consequences of the spurious actuation of the Protection System - Safety Control and Instrumentation Device in all operating modes;
- the justification for holding the plant in a specific mode of operation whilst awaiting reinstatement of the Protection System -Safety Control and Instrumentation Device;
- the potential for permissive signals to compromise diversity in detection of faults;
- the suitability of the categorisation of the permissive functions
- the holistic effects on plant operating procedures; and
- the risks associated with single and common cause failures.

537. I assessed the Basis of Safety Case documents (Ref. 99) (Ref. 100) to determine the use of third party software in the HMI. In 'BSC of Safety Automation System' (Ref. 100) the RP refers to the SAS-SCID as using a third party operating system. The RP has identified the opportunity to work with the developer of the software to assess the software against IEC 61513 (Ref. 21). The RP has committed to pursuing this in site-specific stages. I consider this to be an appropriate level of commitment within GDA. However, since the expectations for the justification of third party software in safety systems are the same as for any software supplied by the RP I consider this is something that should be tracked to resolution; this is addressed by AF-UKHPR1000-0044 (see Section 4.7).

538. Having assessed the submissions provided in response to RO-UKHPR1000-0052 (Ref. 40) I was content that the RP had adequately described the HMI devices employed in the MCR and RSS and provided a suitable and sufficient safety case for GDA. On this basis action 3 of RO-UKHPR1000-0052 was closed (Ref. 252).

539. I sampled the BSCs for the RPS [PS] (Ref. 99), SAS (Ref. 100), KDS [DAS] (Ref. 101), KIC [PCICS] (Ref. 49) and KDA [SA I&C] (Ref. 102) systems for their claims on the HMI systems and found that they now reference their associated HMI and the claims, arguments, and evidence for them. I consider this to be a significant improvement compared to the beginning of Step 4 of GDA as the HMI is now integrated into the UK HPR1000 Centralised C&I safety case.

4.9.2 Strengths

540. The RP has developed safety requirements and design specifications for the Class 1 and Class 2 HMI in the MCR and RSS. The RP has demonstrated that their process for selecting appropriate technologies for HMI systems given the wider system requirements is appropriate.

541. The RP has incorporated the HMI systems in the wider safety case, updating the BSCs so they accurately reflect the need for adequate HMI to achieve their safety functions. The documentation provided is consistent and the rationale provided for the design is sufficiently clear.

4.9.3 Outcomes

542. My assessment of the adequacy of HMI found that the RP had selected appropriate HMI technologies, had integrated HMI design requirements into the overall C&I design process and had provided a suitable and sufficient safety case for the UK HPR1000 HMI equipment. On this basis I was content that RO-UKHPR1000-0052 could be closed.

543. I identified four residual matters that have not been resolved within GDA timescales; these are summarised below:

- Lower Category permissive functions have the potential to interfere with higher Category safety functions on the PS-SCID200.
- Some requirements for the HMI systems do not have clear sources.
- The HMI design specifications appear to be paraphrases of the requirements, not a clear description of how the requirement will be met by the system.
- Third party operating systems have been identified in Class 2 HMI.

These matters have been taken forward as part of Assessment Finding AF-UKHPR1000-0049.

4.9.4 Conclusion

544. Based on the outcome of my assessment of the adequacy of HMI in the UK HPR1000, I have concluded that the HMI aspects of the safety case are sufficiently well developed for the purposes of GDA. I judge the provision of HMI in the MCR and RSS, including the implementation technologies, to be suitable and sufficient, and I am content that the expectations of SAPs ESS.2, ESS.21, ECS.2, EDR.2, EDR.3, ESS.20, ESR.1 and EHF.7 have been adequately addressed given the current stage of design development.

545. I identified shortfalls against the expectations of SAPs ECS.1, ESS.17, ESS.22, and ESS.27. I do not judge these shortfalls to be significant to prevent the issue of a DAC and I have therefore raised Assessment Finding AF-UKHPR1000-0049 for them to be addressed by the licensee.

546. I also identified minor shortfalls against the expectations of SAPs EDR.1 and SC.4, with regard to optioneering studies failing to consider the hazards arising from equipment failures, which I expect the licensee to resolve as part of normal business.

4.10 Justification of Smart Devices

4.10.1 Assessment

547. My assessment of the RP's approach to justification of smart devices considered SAP ESS.27 (Ref. 2) and the guidance provided in NS-TAST-GD-046 (Ref. 10). I also considered SAPs MS.2 and SC.4 in the context of the RP's organisational arrangements for smart device justification.

548. Smart devices are instruments, sensors, actuators or other previously electromechanical components (e.g. relays, valve positioners and controllers) whose functionality is limited and which feature built-in intelligence, in the form of a microprocessor of HDL device, to help perform its function. An important distinction between smart devices and other computer-based systems is that the end user cannot modify device functionality in any way, though they can usually perform limited configuration. In most cases, smart devices are commercial off-the-shelf (COTS) products, or use COTS components, not originally developed to nuclear standards. The use of smart devices in safety and safety-related applications is commonplace, from sensors and actuators to smart devices embedded in equipment and in packaged systems. As such it is an important expectation of GDA that the RP can demonstrate the adequacy of its arrangements for the justification of smart devices for use in nuclear safety applications.

549. During GDA Step 3, the RP presented their 'Methodology of SMART Devices Justification' (Ref. 263). This detailed the RP's approach to justifying smart devices. I assessed this in Step 3 and recorded my findings in my Step 3 assessment note (Ref. 128). I considered this to be broadly aligned with the expectations of NS-TAST-GD-046 (Ref. 10) but there were several outstanding issues which were detailed in RQ-UKHPR1000-0511 (Ref. 109).

550. ONR considers the research undertaken by the Control and Instrumentation Nuclear Industry Forum (CINIF) in the area of smart device justification to be RGP, in particular the EMPHASIS tool which is based on IEC 61508 (Ref. 20) and has been successfully used over several years by nuclear site licensees to assess the PE of COTS smart devices. During GDA Step 4, the RP was unable to gain access to CINIF research and, recognising the need for competence and experience on this topic, engaged the support of an experienced UK based TSC to assist with the further development of its smart device justification methodology.

551. My expectation for the smart device topic for GDA Step 4, which was set out in my assessment plan (Ref. 8), was that the RP demonstrate they have a robust methodology for the justification of smart devices and that the methodology can be practicably implemented.

552. In GDA Step 4 the RP submitted a revised 'Methodology of Smart Devices Substantiation' (Ref. 264), which presents a methodology for assessing production excellence using questionnaires based on IEC nuclear and industrial standards (see paragraphs 562 and 563). The questionnaires against which a device is assessed depends on the requirements of the device to be justified, i.e. the intended classification or use of the device and the standards against which it was developed. The document also details a process which sets out how devices are assessed using these questionnaires, how gaps are addressed by compensating measures, and the selection of ICBMs commensurate with the classification and usage of the device. Finally, the document details how smart devices would be identified in packaged plant. Packaged plant in this document refers to equipment such as heating, ventilation, and air conditioning (HVAC) where the presence of a smart device may not be immediately obvious to a specifying engineer.

553. To demonstrate the implementation of this methodology the RP committed to performing two trial smart device assessments during GDA: one at Class 1 and one at Class 3. These trials were performed with the input of the device manufacturers who contributed to completion of the questionnaires and provided underpinning evidence.

554. As part of the trials, the RP used the questionnaires and identified gaps and proposed compensating measures to resolve those gaps. The RP also identified prospective ICBMs.

555. In 'BSC of Overall I&C Architecture' (Ref. 44) the RP details the CAE relating to the smart device topic. Arguments A2 and A3 of sub-claim C3.1.1.3 broadly state that smart devices used in safety applications will be identified using a systematic process, and that smart devices within C&I systems will be justified according to their safety significance.

556. As of GDA Step 4, no specific smart devices have been identified within the design. This is typical for this stage of the design as component selection would not be expected to take place until site-specific stages. The RP therefore chose to perform the assessment trials on devices that have been selected for use in the reference plant.

4.10.1.1 Justification Methodology

557. I assessed the revised 'Methodology of Smart Device Substantiation' (Ref. 264) and found that it details the RP's methodology for safety justification of smart devices. This includes: the identification of smart devices in packaged plant; the engagement of a suitably qualified and experienced persons (SQEP) assessment team; and the justification of identified devices. The methodology follows the two-legged approach defined in NS-TAST-GD-046 (Ref. 265) with Production Excellence (PE) and ICBMs being separate workstreams which combine to justify the device. I assessed this

document and found that the approach described by the RP is adequate. This is because:

- The methodology uses established UK RGP in the form of international standards to assess the PE of the device, specifically using questionnaires designed by the RP. In my opinion these questionnaires provide an equivalent level of breadth and rigour as established methods used by UK nuclear site licensees, and the overall approach provides a comparable level of confidence.
- The RP has identified an acceptable approach for the identification of compensating measures for the gaps in the PE.
- The RP has developed guidance on the expectations for ICBMs for different safety classes.
- It defines a process for identifying the use of smart devices in package plant;
- it recognises the need of C&I specialist competence when considering smart device qualification.
- It defines the high-level competence requirements.
- It outlines an appropriate justification process with involvement of suitable competence in both the PE and ICBM leg of the justification.
- The PE assessment, compensating measures, and ICBM selection align with the expectations of NS-TAST-GD-046 (Ref. 265).

558. I noted, however, that the methodology does not consider the training needs for smart device assessors, or the skills, knowledge and experience required for the licensee to act as an intelligent customer for the justification of smart devices where they are undertaken by a third party. It is likely that a large number of smart device assessments will have to be performed to support the UK HPR1000. While the RP has considered the competence requirements of the individuals performing specific aspects of smart device justification, this approach must assume sufficient competent resource is available.

559. I raised RQ-UKHPR1000-1024 (Ref. 109) to gain a greater understanding of the RP's training arrangements. My assessment of the RP's response found that while the RP understood that this training would be important there was no intention to formalise the high-level arrangements for training during GDA.

560. I consider this to be an area of risk and a shortfall against the expectations of SAPs SC.4 and MS.2. My expectation is that the safety case should provide the basis for the safe management of people, plant and processes, including training requirements and that the licensee should be able to act as an intelligent customer for smart device assessment. This is a matter that relies upon the management arrangements and choices of the licensee; I have therefore raised Assessment Finding AF-UKHPR1000-0051 for this to be taken forward (see below).

561. I also noted that whilst the RP has presented a process for the identification of smart devices in package plant with responsibilities identified, it is not clear who will own this process in the future. Currently the requirement for system designers to be aware of the smart device justification process only exists within the 'Methodology of Smart Devices Substantiation' (Ref. 264). There is a risk if this requirement is not embedded into wider organisational processes that designers will be unaware of this process and their responsibilities within it, and that smart devices may be unknowingly procured and implemented in safety applications without being justified. This is a matter for the licensee to resolve and is captured in Assessment Finding AF-UKHPR1000-0051 below.

562. I assessed 'Questionnaire for Smart Devices Assessment (F-SC1) Based on IEC Nuclear Standards' (Ref. 266). The questionnaire covers aspects of the standards, such as quality management, lifecycle, hardware, software, and security applicable to Class 1 smart devices. It is based on IEC nuclear standards IEC 61513 (Ref. 21), IEC

60987 (Ref. 17), and IEC 60880 (Ref. 16). The document was not clear as to why these standards had been selected or how the clauses had been chosen. I raised RQ-UKHPR1000-1023 (Ref. 109) to gain an understanding of these gaps. My assessment of the response to RQ-UKHPR1000-1023 found that the RP had explained each of my queries adequately and had provided an example of the review tables used for each of the clauses. The RP subsequently provided a revised version of the questionnaire (Ref. 73) which included clauses from IEC 62566 (Ref. 24). I sampled this update and found that my queries had been addressed in the revised document.

563. I assessed 'Questionnaire for Smart Devices Assessment (F-SC2 and F-SC3) Based on IEC Nuclear Standards' (Ref. 267). This questionnaire covers aspects of the standards IEC 61513 (Ref. 21), IEC 60987 (Ref. 17), IEC 62138 (Ref. 22), and IEC 62566-2 (Ref. 25), as well as aspects of IEC 60880 (Ref. 16) related to cyber security. I sampled the questions in the questionnaire and found that the key aspects of the standards were covered appropriately.

564. I assessed 'Questionnaire for Smart Devices Assessment Based on IEC Industrial Standards' (Ref. 268). This questionnaire relates to the justification of devices at all classes, and covers primarily IEC 61508 (Ref. 20), but also IEC 61513 (Ref. 21), IEC 60987 (Ref. 17), and IEC 60880 (Ref. 16) as aspects such as security and manufacturing are not considered in IEC 61508. The RP therefore elected to supplement with other standards. Having reviewed the questionnaire I was content that appropriate standards had been identified and that the key aspects of the standards were adequately addressed.

565. Combined, I am of the opinion that the questionnaires meet the expectations of NS-TAST-GD-046 (Ref. 265) and present an adequate assessment method of the production excellence of smart devices.

4.10.1.2 Trial Assessments

566. Using the questionnaires, the RP performed trial assessments on two independent smart devices; one at Class 1 and one at Class 3. These trials consisted of a complete PE assessment, recommendation of modifications relating to gaps, assessment of the achievability of justification for the device, and a high-level ICBM strategy.

567. The RP submitted the 'Summary Report for F-SC1 Smart Device Assessment Trial' (Ref. 269). This document details the assessment of a control board for an Uninterruptible Power Supply (UPS) charger. This smart device was assessed using 'Questionnaire for Smart Devices Assessment (F-SC1) Based on IEC Nuclear Standards' (Ref. 266). The summary report details:

- the method of assessment;
- the role of CNPEC;
- the PE assessment of the device;
- the gaps and compensations along with the questions that relate to the gap;
- the prospective ICBMs; and
- a conclusion on the feasibility of the justification of the device.

568. My assessment of this submission found that it gave an overview of the assessment trial performed. As part of my assessment I undertook a sample review of the evidence supporting the assessment trial. As the summary report was not detailed enough to select an appropriate sample, I requested the results of the questionnaire.

569. The RP submitted 'Assessment Table for F-SC1 Smart Device Assessment Trial (Ref. 270)'. This document provided the results of the questionnaire. I used the summary report to target a number of gaps, observations, and passes across the assessment topics. This was to ensure that the breadth of the assessment was sampled. I then

conducted an inspection of the evidence during a technical meeting (Ref. 271). Having sampled the evidence and discussed the RP's judgements I was able to confirm that:

- the RP had actively led the assessments and demonstrated a challenging, questioning attitude, meeting the expectations of the intelligent customer role, and
- the responses to the questionnaire had been appropriate and the reasons provided for the responses aligned with my expectations.

570. I did note some shortfalls against my expectations of how the assessment trial would feedback into the methodology and questionnaire. The RP provided updated versions of the methodology and questionnaire and I was able to confirm that the identified shortfalls had been addressed.

571. Following my inspection of the Class 1 smart device assessment trial, I noted that the conclusions presented in 'Summary Report for F-SC1 Smart Device Assessment Trial' (Ref. 269) did not present a compelling case for why the device would warrant continuation of the full justification methodology, i.e. proceeding with the compensation measures and the ICBMs when the possibility of assessing an alternative device could be pursued. I recognise that whether to pursue the justification of a device following the PE assessment or to seek another device to start the process again will depend on many factors. However, the factors the RP considered were unclear, and I am of the opinion that the decision criteria for this choice should be formalised by the licensee. Therefore, I have raised an Assessment Finding to track this to conclusion.

AF-UKHPR1000-0051 – The licensee shall develop and demonstrate the adequacy of a process for the identification and justification of smart devices. This process shall address the following as a minimum:

- the responsibilities for the identification and justification of smart devices, including in packaged plant;
- the specification of requirements for the use and justification of smart devices;
- the organisational capacity and the skills and experience required for smart device assessors and intelligent customers for smart device justifications; and
- the provision of key points in the process that would allow for decisions to be made as to whether continuation of the justification is warranted.

572. The RP also submitted 'Summary Report for F-SC3 Smart Device Assessment Trial' (Ref. 272). This document details the assessment trial of a smart motor protection relay designed to monitor 3-phase current and voltage and protect against thermal overload given recorded motor history. Similarly to the Class 1 assessment trial summary I requested the assessment tables. 'Assessment Table for F-SC3 Smart Device Assessment Trial' (Ref. 273), developed a sample, and conducted an inspection of the evidence in a technical meeting (Ref. 274). Having sampled the evidence and discussed the RP's judgements I was able to confirm that:

- The RP had actively led the assessments and demonstrated a challenging, questioning attitude, meeting the expectations of the intelligent customer role.
- The responses to the questionnaire had been appropriate and the reasons provided for the responses aligned with my expectations.
- The RP had taken the learning from its Class 1 trial assessment and applied it to the Class 3 assessment, demonstrating a development in the competence relating to PE assessment of smart devices.

573. The RP submitted 'Lessons Learnt from Smart Device Assessment Trial' (Ref. 275). This document details the lessons learnt during the smart device assessment trials with three topics: relationship with the manufacturer, typical gaps and weaknesses, and an overall summary. I assessed this document and consider that it presents a

number of points that were clear from my inspection of the evidence and discussions with the RP. I could not however determine how this document fit within the RP's document structure. The RP explained that this document could be provided to the licensee as part of the safety case handover, however I could not determine any formal process for this. I consider this document to be a useful record of lessons learnt that the licensee could benefit from and I recommend that the RP ensure that the licensee understand its benefits. However, as the RP has already demonstrated a willingness to update their methodology following findings in their trials I consider this matter to be a minor shortfall.

4.10.2 Strengths

574. The RP has developed a smart device justification methodology that meets the expectations of NS-TAST-GD-046 (Ref. 10). Within this methodology the RP has developed a series of questionnaires based on nuclear and industrial standards that present an assessment method of the production excellence of smart devices that achieves an equivalent level of breadth and rigour to that of RGP. The RP have demonstrated through trial assessments that the justification methodology is feasible for Class 1 and Class 3 devices.

4.10.3 Outcomes

575. My assessment of the smart device justification identified two residual matters that were not resolved within GDA timescales; these are summarised below:

- The RP did not provide sufficient information regarding the training strategy for smart device assessors and assessment leads.
- The RP has not established within its organisational procedures a formal process for the identification and justification of smart devices.

576. These have been taken forward as Assessment Finding AF-UKHPR1000-0051.

4.10.4 Conclusion

577. Based on the outcome of my assessment of the smart device justification, I have concluded that the justification methodology is sufficiently well developed for the purposes of GDA, and that the RP has provided an adequate demonstration of its implementation. I am content that, as pertains to the justification of smart devices, the expectations of SAP ESS.27 and NS-TAST-GD-046 have been adequately addressed. I identified shortfalls against the expectations of SAPs SC.4 and MS.2. However, I do not judge these shortfalls to be significant enough to prevent the issue of a DAC and I have therefore raised Assessment Findings for them to be addressed by the licensee.

4.11 Demonstration that Relevant Risks Have Been Reduced to ALARP

4.11.1 Assessment

578. ONR's expectation is that the safety case should demonstrate how risks are reduced so far as reasonably practicable (commonly referred to as ALARP). This expectation is set out in SAP SC.4 (Ref. 2) and further guidance to inspectors is given in technical assessment guide NS-TAST-GD-005 (Ref. 11), including expectations for the development of safety cases in GDA, which can be summarised as follows:

- There should be a clear conclusion that there are no further reasonably practicable improvements that could be implemented, and therefore the risk has been reduced ALARP.
- The RP should identify and justify the codes and standard used.
- The RP should set out the options considered in the evolution of the design and demonstrate that they are appropriate and reduce risks ALARP.

- The RP should undertake risk assessments to demonstrate that improvements as a minimum meet the Basic Safety Objective.

579. Throughout my assessment, as documented in the preceding Sections (4.2 – 546) of this report, I have sought to determine whether specific aspects of the C&I design and safety case meet the expectations of RGP and whether those aspects of the design reduce risks ALARP. I have further discussed the RP's demonstration of compliance with RGP as part of my close-out of RO-UKHPR1000-0016 (Ref. 124). Those aspects of my assessment are not repeated here, and the below paragraphs present a summary of the findings of my assessment of the RP's ALARP demonstration in the C&I topic area.

580. The top-level claims in the C&I safety case, as set out in Chapter 8 of the PCSR (Ref. 3), includes the following claim:

- "Claim I&C-C3 – All reasonably practicable measures are adopted to improve the design of the systems and safety."

581. The principle evidential documentation underpinning this claim that has been considered as part of my assessment is listed below:

- 'ALARP Demonstration Report of PCSR Chapter 8' (Ref. 103).
- 'Suitability Analysis of Codes and Standards in I&C Topic Area' (Ref. 104).

582. I am of the opinion that the RP's approach to demonstrating that relevant risks have been reduced ALARP is reasonable, and that the C&I safety case adequately demonstrates how RGP, in the form or OpEx and international standards and guidance, has been considered in the UK HPR1000 C&I design.

583. Where gaps against RGP are identified I am satisfied that the RP has undertaken suitable and sufficient optioneering studies and has provided adequate justification of the selected options.

584. The ONR TSC raised a number of observations in its reports (Ref. 34) – (Ref. 38) relating to inconsistencies and shortfalls in the C&I safety case. These observations cover areas such as:

- inconsistencies and lack of referencing across the C&I safety case;
- limitations in the argumentation and evidence in the BSCs; and
- dependences on evidence that has not been provided in GDA or which will be developed in subsequent phases.

585. As described in NS-TAST-GD-051 (Ref. 12) ONR's expectation is that the safety case accurately reflects the design, that it is sufficiently clear and that it is supported by evidence. While these shortfalls do not present an impediment to closure of GDA, I am of the opinion that it is important to future phases of design and development that they are resolved. I consider this to be of sufficient importance to be tracked and I have therefore raised an Assessment Finding for this to be addressed by the licensee.

AF-UKHPR1000-0052 – As the detailed design develops, the licensee shall review and update the C&I safety case to ensure that:

- claims and arguments that are dependent on evidence that will be produced in site-specific stages are demonstrated to be met by that evidence;
- gaps in the underpinning evidence are highlighted and resolved;
- evidence is consistently referenced and that there is bi-directional traceability through claims, arguments and evidence and across related areas of the safety case;

- evidence demonstrably supports the claims and arguments against which it is claimed; and
- references to evidential documents are to the latest versions.

586. I have reviewed the PCSR Chapter dedicated to ALARP (Ref. 276) and consider that it provides an accurate representation of the information provided in the 'ALARP Demonstration Report for PCSR Chapter 8' (Ref. 103). For these reasons, I am satisfied that the RP has appropriately considered the ALARP principle in the development of the UK HPR1000 safety case.

4.11.2 Strengths

587. The C&I safety case adequately demonstrates how RGP, in the form or OpEx and international standards and guidance, has been considered in the UK HPR1000 C&I design.

588. Where the RP has identified gaps against RGP it has undertaken suitable and sufficient optioneering studies and has provided adequate justification of the selected options.

4.11.3 Outcomes

589. My assessment of the RP's demonstration that relevant risks have been reduced ALARP did not identify any residual matters additional to those identified elsewhere in this assessment report.

4.11.4 Conclusion

590. Based on the outcome of my assessment of the demonstration that relevant risks have broadly been reduced ALARP and, taking into account the Assessment Findings and minor shortfalls that have been raised, I have concluded that the RP has developed and followed a robust process for the identification of RGP and the evaluation of the design against that RGP.

591. As a result, I am content that the RP has sufficiently addressed the expectations of SAP SC.4 and NS-TAST-GD-005 (Ref. 277) for GDA.

4.12 Consolidated Safety Case

4.12.1 Assessment

592. My assessment of the consolidated safety case has considered SAPs SC.4 and SC.7 (Ref. 2).

593. As stated in Section 41 of this report, the RP provided a production strategy for the C&I topic area (Ref. 105) which set out the document structure and the RP's plan for submissions. This strategy has been revised throughout GDA to capture evolutions in the safety case through the project.

594. The production strategy sets out the strategy for updating the safety case documentation, as follows:

- updates to the PCSR through the project;
- the impact of improvements identified through the RP's processes;
- commitments impacting the safety case in the responses to RQs and ROs;
- commitments impacting the safety case arising from engagements with the regulator; and
- the impact of multi-disciplinary issues.

595. I am satisfied that throughout GDA the RP has managed the update of safety submissions in accordance with this strategy and has routinely issued updates to documentation as it is updated.

596. I undertook a sample review of documentation to satisfy myself that updates arising from the above actions had been adequately reflected in the C&I safety case; my review did not identify any omissions. On the basis of my sample review I judge that necessary clarifications, amendments and additions to evidence have been incorporated into the safety case.

597. As a result, I am satisfied that the C&I aspects of the UK HPR1000 safety case provide a broadly accurate and demonstrably complete reflection for the purposes of GDA.

4.12.2 Strengths

598. The RP has developed a plan to manage the development of the C&I aspects of the UK HPR1000 safety case. Throughout GDA the RP has ensured that the safety case documentation has been updated as the claims, arguments and underpinning evidence have developed.

4.12.3 Outcomes

599. My assessment of the consolidated safety case found that the C&I safety case is representative of the reference design submitted for GDA and incorporates the updates resulting from the activities to address the regulatory queries and observations.

4.12.4 Conclusion

600. Based on the outcomes of my assessment I consider that the C&I aspects of the safety case as set out in Revision H of PCSR Chapter 8, together with the supporting documentation, provides an accurate and complete reflection of the generic UK HPR1000 design at the end of GDA. I am content that the RP has adequately met the expectations of SAPs SC.4 and SC.7 (Ref. 2).

4.13 Comparison with Standards, Guidance and Relevant Good Practice

601. The standards, guidance and relevant good practice which I considered relevant to my assessment of the C&I safety case are identified in sub-section 2.4.3 of this report.

602. Throughout the technical assessment sections of this report, I have documented where my assessment considered the extent of compliance with relevant standards and guidance and have identified where I judge there to be shortfalls that require resolution.

603. In general, I am satisfied that the RP has appropriately identified the codes, standards and RGP that are relevant to the UK HPR1000 C&I design and safety case and has provided a suitable and sufficient justification for their applicability in ‘Suitability Analysis of Codes and Standards in I&C Topic Area’ (Ref. 104). Where specific shortfalls in compliance have been identified I have raised Assessment Findings for these to be addressed by the licensee.

5 CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

604. This report presents the findings of my C&I assessment of the generic UK HPR1000 design as part of the GDA process.

605. Based on my assessment, undertaken on a sampling basis, I have concluded the following:

- The C&I safety case, comprising the PCSR, supporting Basis of Safety Case documents and the underpinning evidential documentation, has been adequately developed for the purposes of GDA.
- The C&I architecture is consistent with international guidance and has been adequately substantiated for the purposes of GDA.
- The RP has identified significant shortfalls in the adequacy of production excellence of the FirmSys platform against the expectations of safety Class 1 and has developed a suitable programme of work to address these shortfalls.
- The development of the hardware-based platform for the secondary protection system provides adequate diversity between different layers of defence in the C&I architecture.
- The RP has identified appropriate standards against which the centralised C&I systems will be designed and has identified compensating measures to resolve shortfalls that were revealed by compliance analysis. However, significant further work is required to complete the safety justification of the C&I platforms and systems.
- There is a lack of clarity and traceability in the specification of requirements across all C&I platforms and systems.
- From a C&I perspective I am satisfied that, given the early stage of design, the RP has given adequate consideration to the management and control of cyber-security risks.
- The HMI aspects of the C&I safety case are sufficiently well developed for the purposes of GDA.
- The RP has developed a suitable and sufficient methodology for the safety justification of smart devices and has demonstrated that this methodology can be practicably implemented.
- Noting the 24 Assessment Findings and nine minor shortfalls raised in my assessment, I am satisfied that the expectations of ONR's Safety Assessment Principles and Technical Assessment Guides are met in generic UK HPR1000 design.

606. Overall, based on my sample assessment of the safety case for the generic UK HPR1000 design undertaken in accordance with ONR's procedures, I am satisfied that the case presented within the PCSR and supporting documentation is adequate. On this basis, I am content that a DAC should be granted for the generic UK HPR1000 design from a C&I perspective.

5.2 Recommendations

607. Based upon my assessment detailed in this report, I recommend that:

- **Recommendation 1**: From a C&I perspective, ONR grant a DAC for the generic UK HPR1000 design.

- **Recommendation 2**: The 24 Assessment Findings identified in this report should be resolved by the licensee for a site specific application of the generic UK HPR1000 design.

6 REFERENCES

1. *New nuclear reactors: Generic Design Assessment: Guidance to Requesting Parties for the UK HPR1000,* ONR-GDA-GD-001, Revision 4, October 2019, ONR. www.onr.org.uk/new-reactors/ngn03.pdf
2. *Safety Assessment Principles for Nuclear Facilities. 2014 Edition,* Revision 1, January 2020, ONR. http://www.onr.org.uk/saps/saps2014.pdf
3. *UKHPR1000 GDA Project. Pre-Construction Safety Report. Chapter 8. Instrumentation and Control,* HPR/GDA/PCSR/0008, Revision 2, July 2021, CGN. [CM9 Ref. 2021/48484]
4. *Guidance on the Mechanics of Assessment,* Revision 0, April 2020, ONR. https://www.onr.org.uk/operational/tech_asst_guides/index.htm
5. *Security Assessment Principles for the Civil Nuclear Industry. 2017 Edition,* Version 0, March 2017, ONR. www.onr.org.uk/syaps/security-assessment-principles-2017.pdf
6. *Technical Assessment Guides,* , ONR. https://www.onr.org.uk/operational/tech_asst_guides/index.htm
7. *Step 4 Cyber Security & Information Assurance Assessment of the UK HPR1000 Reactor,* ONR-NR-AN-21-014, Revision 0, July 2021, ONR. [CM9 Ref. 2021/44510]
8. *GDA Step 4 Assessment Plan of Control and Instrumentation topic for the UK HPR1000 Reactor,* ONR-GDA-UKHPR1000-AP-19-004, Revision 0, February 2020, ONR. [CM9 Ref. 2019/374782]
9. *Safety Systems,* NS-TAST-GD-003, Revision 9, March 2018, ONR. https://www.onr.org.uk/operational/tech_asst_guides/index.htm
10. *Computer Based Safety Systems,* NS-TAST-GD-046, Revision 6, April 2019, ONR. [CM9 Ref. 2020/261582]
11. *Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable),* NS-TAST-GD-005, Revision 11, November 2020, ONR. https://www.onr.org.uk/operational/tech_asst_guides/index.htm
12. *The Purpose, Scope, and Content of Safety Cases,* NS-TAST-GD-051, Revision 7, December 2019, ONR. www.onr.org.uk/operational/tech_asst_guides/index.htm [CM9 Ref. 2020/284313]
13. *Categorisation of Safety Functions and Classification of Structures and Components,* NS-TAST-GD-094, Revision 2, July 2019, ONR. https://www.onr.org.uk/operational/tech_asst_guides/index.htm
14. *Nuclear Power Plants. Instrumentation and Control Important to Safety. Separation,* BS EN 60709:2019, July 2019, BSI.
15. *Nuclear Power Plants. Instrumentation and Control Important to Safety. Qualification,* BS EN 60780-323:2017, March 2016, BSI.
16. *Nuclear Power Plants. Instrumentation and Control Important to Safety. Software Aspects for Computer-based Systems Performing Category A Functions,* BS EN 60880:2009, January 2010, BSI.
17. *Nuclear Power Plants. Instrumentation and Control Important to Safety. Hardware Design Requirments for Computer-based Systems,* BS EN 60987:2015, April 2015, BSI.
18. *Nuclear Power Plants. Instrumentation, control and electrical power systems important to safety. Categorisation of functions and classification of systems,* BS EN 61226: 2010, September 2009, BSI.
19. *Nuclear Power Plants. Instrumentation and control systems important to safety. Data communication in systems performing category A functions,* BS EN IEC 61500:2019, July 2019, BSI.
20. *Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-related Systems,* BS EN 61508, June 2010, BSI.

21. *Nuclear Power Plants. Instrumentation and Control Important to Safety. General Requirements for Systems,* BS EN 61513:2013, March 2013, British Standards Institute (BSI).
22. *Nuclear Power Plants. Instrumentation and Control Important to Safety. Software Aspects for Computer Based Systems Performing Category B or C Functions,* BS EN 62138:2019, October 2019, BSI.
23. *Nuclear Power Plants. Instrumentation and control systems important to safety. Requirements for coping with common cause failure,* BS EN 62340:2008, March 2008, BSI.
24. *Nuclear power plants. Instrumentation and control important to safety. Development of HDL-programmed integrated cicruits for systems performing category A functions,* IEC 62566, 2012, International Electrotechnical Commission.
25. *Nuclear power plants. Instrumentation and control important to safety. Developement of HDL-programmed integrated circuits for systems performing category B or C functions,* IEC 62566-2, 2020, International Electrotechnical Commision.
26. *Nuclear Power Plants. Instrumentation, Control and Electrical Power Systems. Cybersecurity Requirements,* BS IEC 62645:2020, November 2019, BSI.
27. *Nuclear Power Plants. Instrumentation and Control Systems. Requirments for Cooddinating Safety and Cybersecurity,* BS IEC 62859:2016, March 2016, BSI.
28. *Information Technology. Security Techniques. Information Security Risk Management,* ISO/IEC 27005:2018, July 2018, International Electrotechnical Commission (IEC).
29. *IAEA Safety Standards. Safety Classification of Structures, Systems and Components in Nuclear Power Plants,* Safety Specific Guide No SSG-30, May 2014, International Atomic Energy Agency (IAEA). www.iaea.org
30. *IAEA Safety Standards. Design of Instrumtnation and Control Systems of Nuclear Power Plants,* Specific Safety Guide No SSG-39, April 2016, IAEA. www.iaea.org
31. *ONR TSC C&I Support for General Nuclear Systems UK HPR1000 GDA Step 3 - Adequacy of C&I Architecture,* S_P1893_041_02, 1.1, January 2020, Altran. [CM9 Ref. 2020/47074]
32. *ONR TSC C&I Support for General Nuclear Systems UK HPR1000 GDA Step 3 - Confirmation of Adequacy of Platforms Step 3,* S_P1893_041_04, 1.1, January 2020, Altran. [CM9 Ref. 2020/47084]
33. *ONR TSC C&I Support for General Nuclear Systems UK HPR1000 GDA Step 3 - Confirmation of the Adequacy of the Systems,* S_P1893_041_05, 1.1, January 2020, Altran. [CM9 Ref. 2020/47070]
34. *ONR TSC C&I Support for General Nuclear Systems UK HPR1000 GDA Step 4 - Structure and Clarity of the C&I Safety Case,* S.P1893.041.06, 1.0, August 2021, Capgemini. [CM9 Ref. 2021/60559]
35. *ONR TSC C&I Support for General Nuclear Systems UK HPR1000 GDA Step 4 - Evidence and Adequacy of C&I Architecture,* S.P1893.041.07, 1.0, July 2021, Capgemini Engineering. [CM9 Ref. 2021/60562]
36. *ONR TSC C&I Support for General Nuclear Systems UK HPR1000 GDA Step 4 - Evidence and Adequacy of C&I Architecture - Appendix A Cyber Security,* S.P1893.041.07 - Appendix A, Issue 1.0, August 2021, Capgemini Engineering. [CM9 Ref. 2021/60561]
37. *ONR TSC C&I Support for General Nuclear Systems UK HPR1000 GDA Step 4 - Confirmation of Adequacy of Platforms,* S.P1893.041.08, 1.0, August 2021, Capgemini Engineering. [CM9 Ref. 2021/60563]
38. *ONR TSC C&I Support for General Nuclear Systems UK HPR1000 GDA Step 4 - Confirmation of the Adequacy of the Systems,* S.P1893.041.09, 1.0, August 2021, Capgemini Engineering. [CM9 Ref. 2021/60557]
39. *Email from TSC to DF RE: RO-52 closure support,* email, April 2021, Altran. [CM9 Ref. 2021/52033]

40. *UKHPR1000 - Regulatory Observation (RO) Tracking Sheet,* , ONR. [CM9 Ref. 2017/465031]
41. *Assessment of Response to RO-UKHPR1000-0039 - Performance Analysis of UK HPR1000 Heating Ventilation and Air Conditioning Systems,* ONR-NR-AN-21-030, Revision 0, July 2021, ONR. [CM9 Ref. 2021/49521]
42. *Assessment of the Response to RO-UKHPR1000-0013 - Modelling of Computer-Based System Reliability in the PSA,* ONR-NR-AN-20-01, Revision 0, December 2020, ONR. [CM9 Ref. 2020/320651]
43. *Assessment of the Response to RO-UKHPR1000-0056 - Fuel Route Safety Case,* ONR-NR-AN-21-054, Revision 0, September 2021, ONR. [CM9 Ref. 2021/70093]
44. *BSC of Overall I&C Architecture,* GHX06002001DIYK01GN, Revision F, May 2021, General Nuclear Systems Ltd. [CM9 Ref. 2021/51810]
45. *BSC of Protection System,* GHX06002002DIYK03GN, Revision G, June 2021, CGN. [CM9 Ref. 2021/51813]
46. *BSC of Safety Automation System,* GHX06002003DIYK03GN, Revision D, June 2021, CGN. [CM9 Ref. 2021/51437]
47. *BSC of Diverse Actuation System,* GHX06002013DIYK03GN, Revision D, jUNE 2021, CGN. [CM9 Ref. 2021/51453]
48. *BSC of Plant Standard Automation System,* GHX06002004DIYK03GN, Revision C, March 2021, CGN. [CM9 Ref. 2021/26036]
49. *BSC of Plant Computer Information and Control System,* GHX06120010DIKX03GN, Revision D, January 2021, CGN. [CM9 Ref. 2021/8470]
50. *BSC of Severe Accident I&C System,* GHX06002005DIYK03GN, Revision D, June 2021, CGN. [CM9 Ref. 2021/51444]
51. *Topic Report of FirmSys Platform,* GHX56100001GSNS44TR, Revision D, June 2021, CGN. [CM9 Ref. 2021/51489]
52. *Topic Report of HOLLiAS-N Platform,* GHX56100002GSNS44TR, Revision A, July 2019, CGN. [CM9 Ref. 2019/227688]
53. *Topic Report of SpeedyHold Platform,* GHX5600003GNS44TR, Revision A, July 2019, CGN. [CM9 Ref. 2019/229997]
54. *UK HPR1000 Overall I&C Design Specification,* GHX06002021DIYK03GN, Revision D, April 2021, CGN. [CM9 Ref. 2021/35862]
55. *Independence Analysis of I&C Systems,* GHX06002020DIYK03GN, Revision E, June 2021, CGN. [CM9 Ref. 2021/51854]
56. *Defence in Depth and Diversity Analysis Report,* GHX06002014DIYK03GN, B, November 2020, CGN. [CM9 Ref. 2020/316497]
57. *Centralised I&C System Reliability Study Report,* GHX06002026DIYK03GN, Revision B, April 2021, CGN. [CM9 Ref. 2021/35017]
58. *RPS [PS] System Requirements Specification,* GHX06002018DIYK03GN, Revision E, May 2021, CGN. [CM9 Ref. 2021/43596]
59. *SAS System Requirements Specification,* GHX06100005DIYK03GN, Revision E, June 2021, CGN. [CM9 Ref. 2021/51469]
60. *KDS [DAS] System Requirements Specification,* GHX06002022DIYK03GN, Revision E, June 2021, CGN. [CM9 Ref. 2021/51457]
61. *PSAS System Requirements Specification,* GHX06100004DIYK03GN, Revision D, March 2021, CGN. [CM9 Ref. 2021/26041]
62. *KIC [PCICS] System Requirements Specification,* GHX06120002DIKX03GN, Revision D, January 2021, CGN. [CM9 Ref. 2021/8308]
63. *KDA [SA I&C] System Requirements Specification,* GHX06002012DIYK03GN, Revision D, March 2021, CGN. [CM9 Ref. 2021/26037]

64. *KDA [SA I&C] System Requirements Specification,* GHX06002012DIYK03GN, Revision E, June 2021, CGN. [CM9 Ref. 2021/51450]
65. *Design Specification of RPS [PS],* GHX56100018GSNS44TR, Revision E, June 2021, CGN. [CM9 Ref. 2021/51498]
66. *Design Specification of Safety Automation System (SAS),* GHX56100026GSNS44TR, Revision E, June 2021, CGN. [CM9 Ref. 2021/51502]
67. *Technical Requirements Specification for Diverse Actuation System (KDS [DAS]) Platform,* GHX56100023GSNS44TR, Revision C, January 2021, CGN. [CM9 Ref. 2021/8289]
68. *Design Specification of Plant Standard Automation System (PSAS),* GHX56100027GSNS44TR, Revision D, April 2021, CGN. [CM9 Ref. 2021/30054]
69. *Design Specification of KIC [PCICS],* GHX56100045GSNS44TR, Revision D, February 2021, CGN. [CM9 Ref. 2021/12199]
70. *Design Specification of Severe Accident System,* GHX56100028GSNS44TR, Revision E, June 2021, CGN. [CM9 Ref. 2021/51506]
71. *Demonstration of Production Excellence for FirmSys Platform,* GHX56100036GSNS44TR, Revision B, May 2020, CGN. [CM9 Ref. 2020/159500]
72. *Assessment Report of Production Excellence for FirmSys Platform,* GHX56100185GSNS44TR, Revision B, April 2021, CGN. [CM9 Ref. 2021/35018]
73. *Demonstration of Production Excellence for the RPS [PS],* GHX56100037GSNS44TR, Revision D, June 2021, CGN. [CM9 Ref. 2021/51849]
74. *Demonstration of Production Excellence for the SAS,* GHX56100038GSNS44TR, Revision D, June 2021, CGN. [CM9 Ref. 2021/51847]
75. *Demonstration of Production Excellence for HOLLiAS-N,* GHX56100054GSNS44TR, Revision A, June 2020, CGN. [CM9 Ref. 2020/195712]
76. *Demonstration of Production Excellence for the PSAS and KIC [PCICS],* GHX56100053GSNS44TR, Revision D, June 2021, CGN. [CM9 Ref. 2021/51812]
77. *Demonstration of Production Excellence for SpeedyHold Platform,* GHX56100067GSNS44TR, Revision B, April 2021, CGN. [CM9 Ref. 2021/35867]
78. *Demonstration of Production Excellence for the KDA [SA I&C],* GHX56100068GSNS44TR, Revision D, June 2021, CGN. [CM9 Ref. 2021/51850]
79. *Strategy for Conducting ICBMs Activities for RPS [PS],* GHX06100015DIYK03GN, Revision D, June 2021, CGN. [CM9 Ref. 2021/51474]
80. *Strategy for Conducting ICBMs Activities for SAS,* GHX06100001DIYK03GN, Revision D, June 2021, CGN. [CM9 Ref. 2021/51464]
81. *Strategy for Conducting ICBMs Activities for PSAS and KIC [PCICS],* GHX06100021DIYK03GN, Revision D, June 2021, CGN. [CM9 Ref. 2021/51488]
82. *Strategy for Conducting ICBMs Activities for KDA [SA I&C],* GHX06100020DIYK03GN, Revision D, June 2021, CGN. [CM9 Ref. 2021/51481]
83. *FirmSys Platform Compliance Analysis with IEC 60880,* GHX56100011GSNS44TR, Revision B, June 2020, CGN. [CM9 Ref. 2020/195760]
84. *FirmSys Platform Compliance Analysis with IEC 60987,* GHX56100012GSNS44TR, Revision C, December 2020, CGN. [CM9 Ref. 2021/273]
85. *HOLLiAS-N Platform Compliance Analysis with IEC 62138,* GHX56100013GSNS44TR, Revsion B, August 2020, CGN. [CM9 Ref. 2020/256943]
86. *SpeedyHold Platform Compliance Analysis with IEC 62138,* GHX56100014GSNS44TR, Revision B, August 2020, CGN. [CM9 Ref. 2020/256944]
87. *Comparison Analysis of FirmSys Based I&C Systems with IEC 60987,* GHX56100032GSNS44TR, Revision A, September 2020, CGN. [CM9 Ref. 2020/286790]

88. *Comparison of UK HPR1000 Protection System RPS [PS] with IEC 61513,* GHX00630002DIYK03GN, Revision A, August 2019, CGN. [CM9 Ref. 2019/251265]
89. *Comparison Analysis of Protection System (RPS [PS]) with IEC 60880,* GHX56100041GSNS44TR, Revision A, September 2020, CGN. [CM9 Ref. 2020/286780]
90. *Comparison of UK HPR1000 Safety Automation System SAS with IEC 61513,* GHX06100014DIYK03GN, Revision A, April 2020, CGN. [CM9 Ref. 2021/126406]
91. *Comparison Analysis of Safety Automation System (SAS) with IEC 62138,* GHX56100042GSNS44TR, Revision A, September 2020, CGN. [CM9 Ref. 2020/286784]
92. *Comparison of UK HPR1000 PSAS and KIC [PCICS] with IEC 61513,* GHX06100022DIYK03GN, Revision A, May 2020, CGN. [CM9 Ref. 2020/159436]
93. *Comparison Analysis of PSAS and KIC [PCICS] with IEC 62138,* GHX56100044GSNS44TR, Revision A, October 2020, CGN. [CM9 Ref. 2020/303849]
94. *Comparison of UK HPR1000 Severe Accident System with IEC 61513,* GHX06100024DIYK03GN, Revision A, May 2020, CGN. [CM9 Ref. 2020/159443]
95. *Comparison Analysis of Severe Accident I&C System (KDA [SA I&C]) with IEC 62138,* GHX56100043GSNS44TR, Revision A, October 2020, CGN. [CM9 Ref. 2020/303851]
96. *An Example of Component Level FMEA Report on FirmSys Platform,* GHX56100181GSNS44TR, Revision A, Janaury 2021, CGN. [CM9 Ref. 2021/8478]
97. *The Failure Modes and Effect Analysis (FMEA) of KDS [DAS],* GHX56100064GSNS44TR, Revision A, August 2020, CGN. [CM9 Ref. 2020/256941]
98. *Justification of Non-interference of Safety Functions in KDS [DAS],* GHX56100180GSNS44TR, Revision A, January 2021, CGN. [CM9 Ref. 2021/8281]
99. *BSC of Protection System,* GHX06002002DIYK03GN, Revision F, May 2021, General Nuclear Systems Ltd. [CM9 Ref. 2021/43594]
100. *BSC of Safety Automation System,* GHX06002003DIYK03GN, Revision C, January 2021, CGN. [CM9 Ref. 2021/8514]
101. *BSC of Diverse Actuation System,* GHX06002013DIYK03GN, Revision C, January 2021, CGN. [CM9 Ref. 2021/8465]
102. *BSC of Severe Accident I&C System,* GHX06002005DIYK03GN, Revision C, March 2021, CGN. [CM9 Ref. 2021/27289]
103. *ALARP Demonstration Report of PCSR Chapter 8,* GHX00100051KPGB03GN, Revision F, April 2021, CGN. [CM9 Ref. 2021/35841]
104. *Suitability Analysis of Codes and Standards in I&C Topic Area,* GHX00800006DIYK02GN, Revision C, May 2020, CGN. [CM9 Ref. 2020/316455]
105. *Production Strategy for Instrumentation and Control,* GHX00100023KPGB03GN, Revision F, April 2021, CGN. [CM9 Ref. 2021/34406]
106. *SAS System Requirements Specification,* GHX06100005DIYK03GN, Revision D, January 2021, CGN. [CM9 Ref. 2021/8315]
107. *UKHPR1000 GDA Project. Pre-Construction Safety Report. Chapter 8. Instrumentation and Control,* HPR/GDA/PCSR/0008, Revision 1, January 2020, CGN. [CM9 Ref. 2020/13661]
108. *BSC of Overall I&C Architecture,* GHX06002001DIYK01GN, Revision B, September 2018, CGN. [CM9 Ref. 2018/318225]
109. *UK HPR1000 - Regulatory Query (RQ) Tracking Sheet,* , ONR. [CM9 Ref. 2017/407871]
110. *Contact Record. UK HPR1000 GDA Step 3. Control & Instrumentation Level 4 Workshop in China,* ONR-NR-CR-18-790, Revision 0, March 2019, ONR. [CM9 Ref. 2019/87037]
111. *BSC of Overall I&C Architecture,* GHX06002001DIYK01GN, Revision C, May 2019, CGN. [CM9 Ref. 2019/152717]

112. *BSC of Protection System,* GHX06002002DIYK03GN, Revision B, April 2019, CGN. [CM9 Ref. 2019/127426]
113. *BSC of Diverse Actuation System,* GHX06002013DIYK03GN, Revision A, July 2019, CGN. [CM9 Ref. 2019/229947]
114. *FMEA Report of Protection System,* GHX56100017GSNS44TR, Revision A, April 2019, CGN. [CM9 Ref. 2019/124198]
115. *Independence Analysis of I&C Systems,* GHX06002020DIYK03GN, Revision A, January 2019, CGN. [CM9 Ref. 2019/27469]
116. *Contact Record. GDA I&C Workshop. CAE Discussion. Level 4,* ONR-NR-CR-20-162, Revision 0, May 2020, ONR. [CM9 Ref. 2020/164811]
117. *BSC of Overall I&C Architecture,* GHX06002001DIYK01GN, Revision D, November 2020, CGN. [CM9 Ref. 2020/316457]
118. *BSC of Protection System,* GHX06002002DIYK03GN, Revision D, November 2020, General Nuclear Systems Ltd. [CM9 Ref. 2020/316499]
119. *BSC of Safety Automation System,* GHX06002003DIYK03GN, Revision B, November 2020, CGN. [CM9 Ref. 2020/316454]
120. *BSC of Diverse Actuation System,* GHX06002013DIYK03GN, Revision B, November 2020, CGN. [CM9 Ref. 2020/316514]
121. *BSC of Plant Standard Automation System,* GHX06002004DIYK03GN, Revision B, November 2020, CGN. [CM9 Ref. 2020/216465]
122. *BSC of Plant Computer Information and Control System,* GHX06120010DIKX03GN, Revision C, November 2020, CGN. [CM9 Ref. 2020/316486]
123. *BSC of Severe Accident I&C System,* GHX06002005DIYK03GN, Revision B, November 2020, CGN. [CM9 Ref. 2020/316476]
124. *Assessment of the Response to RO-UKHPR1000-0016 - Demonstration of Compliance with Relevant Good Practice,* ONR-NR-AN-21-025, Revision 0, June 2021, ONR. [CM9 Ref. 2021/29159]
125. *Impact Analysis for Changes of UNIT3&4 FirmSys Safety-class Products on Qualification Result,* GHX56100077GSNS44TR, Revision A, June 2020, CTEC. [CM9 Ref. 2020/195715]
126. *Modification Form for Diversity Improvement for Protection Parameters,* HPR-GDA-LETT-0076, Revision 0, October 2020, CGN. [CM9 Ref. 2020/304379]
127. *UK HPR1000 Overall I&C Architecture Diagram,* GHX00100001DIYK00GN, C, November 2020, CGN. [CM9 Ref. 2020/316458]
128. *GDA Step 3 Assessment of Control and Instrumentation for the UK HPR1000 Reactor,* ONR-NR-AN-19-009, Revision 0, January 2020, ONR. [CM9 Ref. 2019/345223]
129. *Methodology of Safety Categorisation and Classification,* GHX00100062DOZJ03GN, Revision B, June 2018, CGN. [CM9 Ref. 2018/199731]
130. *Functional Assignment of I&C Systems,* GHX06100003DIYK03GN, Revision A, December 2019, CGN. [CM9 Ref. 2020/119]
131. *UK HPR1000 Fault Schedule,* GHX00600276DRAF02GN, Revision D, January 2021, CGN. [CM9 Ref. 2021/8482]
132. *UK HPR1000 - Step 4 Fault Studies Assessment Report,* ONR-NR-AR-21-014, 0, December 2021, ONR. [CM9 Ref. 2021/44803]
133. *RPN - Nuclear Instrumentation System Design Manual Chapter 3 System Functions and Design Bases,* GHX17RPN002DIYK45GN, Revision C, September 2021, CGN. [CM9 Ref. 2021/66561]
134. *KRT - Plant Radiation Monitoring System Design Manual Chapter 4 System and Component Design,* GHX17KRT004DIYK45GN, Revision E, May 2021, CGN. [CM9 Ref. 2020/161866]

135. *RIC - In-core Instrumentation System Design Manual Chapter 3 System Functions and Design Bases,* GHX17RIC003DIYK45GN, Revision C, August 2020, CGN. [CM9 Ref. 2020/23308]
136. *Step 4 Assessment of Fuel and Core Design for the UK HPR1000 Reactor,* ONR-NR-AR-21-021, Revision 0, November 2021, ONR. [CM9 Ref. 2021/23724]
137. *Modification Form - Self Powered Neutron Detector (SPND) Sub-system Category,* M58-GHTCN000173-B, Revision B, November 2020, CGN. [CM9 Ref. 2020/312196]
138. *RIC [IIS] - In-core Instrumentation System Design Manual Chapter 3 System Functions and Design Bases,* GHX17RIC003DIYK45GN, Revision D, September 2021, CGN. [CM9 Ref. 2021/66557]
139. *RGL [RPICS] - Rod Position Indication and Rod Control System Design Manual Chapter 3 System Functions and Design Bases,* GHX17RGL003DIYK45GN, Revision D, September 2021, CGN. [CM9 Ref. 2021/66553]
140. *Reliability Targets of the I&C Systems for UK HPR1000,* GHX06001015DIYK03GN, Revision D, November 2020, CGN. [CM9 Ref. 2020/316459]
141. *Centralised I&C System Reliability Study Report,* GHX06002026DIYK03GN, Revision A, October 2020, CGN. [CM9 Ref. 2020/304846]
142. *Independence Analysis of I&C Systems,* GHX06002020DIYK03GN, Revision D, January 2021, CGN. [CM9 Ref. 2021/8458]
143. *Optioneering Analysis Report for CIM Improvement,* GHX06002024DIYK03GN, Revision B, September 2020, CGN. [CM9 Ref. 2020/288639]
144. *Optioneering Analysis Report for SPM Improvement,* GHX06100009DIYK03GN, Revision B, January 2021, CGN. [CM9 Ref. 2021/8320]
145. *Assessment of the Response to RO-UKHPR1000-0017 - Demonstration of Independence Between C&I Systems,* ONR-AN-AN-21-032, Revision 0, June 2021, ONR. [CM9 Ref. 2021/40150]
146. *Diversity Improvement for Protection Parameters,* M37-GHTCN000125, Revision A, October 2020, CGN. [CM9 Ref. 2020/304379]
147. *Functional Analysis Report for Diverse Protection Line Design,* GHX00100130DOZJ03GN, Revision A, March 2020, CGN. [CM9 Ref. 2020/82963]
148. *Optioneering Report on Safety Injection Signal in SBLOCA,* GHX00100058DRAF03GN, Revision A, April 2020, CGN. [CM9 Ref. 2020/128289]
149. *Optioneering on VVP [MSS] Related to the Loss of MSL Isolation Induced by CCF under SGTR (one tube),* GHX00100070DNHX03GN, Revision B, August 2020, CGN. [CM9 Ref. 2020/233049]
150. *Optioneering on PTR [FPCTS] Related to the Loss of Isolation Induced by CCF Under Isolabe Piping Break,* GHX00100071DDNHX03GN, Revision C, August 2020, CGN. [CM9 Ref. 2020/233178]
151. *RPS [PS] System Requirements Specification,* GHX06002018DIYK03GN, Revision D, January 2021, CGN. [CM9 Ref. 2021/8312]
152. *Justification for Diverse Protection Line Design on HVAC System,* GHX08000004DCNT03TR, Revision B, May 2020, CGN. [CM9 Ref. 2020/163994]
153. *Optioneering Report of HVAC System Due to Diverse Protection Line Design Requirement,* GHX08000006DCNT03TR, Revision C, November 2020, CGN. [CM9 Ref. 2020/314101]
154. *Modification Form - Cat1 - HVAC systems diversity modification,* M35-GHTCN000127, Revision A, October 2020, . [CM9 Ref. 2020/304330]
155. *UK HPR1000 - GDA Step 4 Mechanical Engineering Assessment Report,* ONR-NR-AR-21-004, Revision 0, December 2021, ONR. [CM9 Ref. 2021/53696]
156. *UK HPR1000 GDA Step 4 – Electrical and C&I Engineering Level 4 Meeting,* ONR-NR-CR-19-573, Revision 0, March 2020, ONR. [CM9 Ref. 2020/77087]

157. *UK HPR1000 - Step 4 Electrical Engineering Assessment Report,* ONR-NR-AR-21-011, Revision 0, January 2022, ONR. [CM9 Ref. 2021/51507]
158. *Modification Delivery Form, Modification of CIM Design,* M30-GHTCN000116., Revision A, November 2020, CGN. [CM9 Ref. 2020/304360]
159. *Modification Delivery Form, Modification of SPM Design,* M90-GHTC000201, Revision A, April 2021, CGN. [CM9 Ref. 2021/31032]
160. *Internal Fire Safety Assessment Report for Reactor Building,* GHX84200041DOZJ03GN, Revision A, June 2020, CGN. [CM9 Ref. 2020/164044]
161. *Internal Fire Safety Assessment Report for Safeguard Buildings,* GHX84200035DOZJ03GN, Revision A, February 2020, CGN. [CM9 Ref. 2020/65928]
162. *Internal Electromagnetic Interference Safety Assessment Report,* GHX84200002SATK03GN, Revision A, June 2020, CGN. [CM9 Ref. 2020/200839]
163. *BSC of Protection System,* GHX06002002DIYK03GN, Revision E, January 2021, CGN. [CM9 Ref. 2021/8433]
164. *Methodology of PIE Identification,* GHX00100008DOZJ03GN, Revision H, January 2019, CGN. [CM9 Ref. 2019/26887]
165. *PIE List of Spurious Actuation for I&C Systems,* GHX00100003DIYK03GN, Revision C, September 2019, CGN. [CM9 Ref. 2019/282603]
166. *Common Position on Spurious Actuation,* CP-DICWG-13, July 2017, MDEP. https://www.oecd-nea.org/mdep/common-positions/cp-dicwg-13.pdf
167. *PIE Bounding Process of Spurious I&C Actuation,* GHX00100009DRAF03GN, Revision C, October 2020, CGN. [CM9 Ref. 2020/305445]
168. *Analysis for Spurious I&C Actuation Events,* GHX00600348DRAF02GN, Revision B, October 2020, CGN. [CM9 Ref. 2020/305433]
169. *Assessment of the Response to RO-UKHPR1000-0002 - Demonstration that the UK HPR1000 Design is Suitably Aligned with the Generic Site Envelope,* ONR-NR-AN-20-018, Revision 0, June 2021, ONR. [CM9 Ref. 2021/5087]
170. *UK HPR1000 - Step 4 External Hazards Assessment Report,* ONR-NR-AR-21-006, Revision 0, November 2021, ONR. [CM9 Ref. 2021/46598]
171. *Space Weather Safety Evaluation Report,* GHX86000002DOZJ00GN, Revision A, October 2020, CGN. [CM9 Ref. 2020/304100]
172. *UK HPR1000 - Assessment of the Response to RO-UKHPR1000-021 – Demonstration of the Adequacy of Examination, Maintenance, Inspection and Testing (EMIT) of Structures, Systems, and Components Important to Safety,* ONR-NR-AN-21-004, Revision 0, May 2021, ONR. [CM9 Ref. 2021/41436]
173. *Examination, Maintenance, Inspection and Testing (EMIT) Strategy,* GHX42EMT001DOYX45GN, Revision C, July 2020, CGN. [CM9 Ref. 2020/225864]
174. *Examination, Maintenance, Inspection and Testing (EMIT) Windows,* GHX42EMT002DOYX45GN, Revision D, January 2021, CGN. [CM9 Ref. 2021/8441]
175. *EMIT Consistency Analysis,* GHX42EMT004DOYX45GN, Revision A, September 2020, CGN. [CM9 Ref. 2020/289528]
176. *UK HPR1000 GDA - ONR email - C&I input to assessment of RO-UKHPR1000-0021,* May 2021, ONR. [CM9 Ref. 2021/66943]
177. *UK HPR1000 Overall I&C Integration Test Plan,* GHX06100025DIYK03GN, Revision A, October 2020, CGN. [CM9 Ref. 2020/304851]
178. *Commissioning Strategy for I&C Systems,* GHX06002001DIYK45GN, Revision A, November 2019, CGN. [CM9 Ref. 2019/354882]
179. *Product Excellence Summary Paper for the CPLD-based Watchdog Circuit of FirmSys,* GHX56100163GSNS44TR, Revision A, November 2020, CGN. [CM9 Ref. 2020/316469]

180. *Product Excellence Summary Paper for Software Self-diagnostics Function of FirmSys,* GHX56100155GSNS44TR, Revision A, August 2020, CGN. [CM9 Ref. 2020/254193]
181. *Product Excellence Summary Paper for HNU DP-RAM Circuit of FirmSys,* GHX56100168GNSS44TR, Revision A, November 2020, CGN. [CM9 Ref. 2020/316592]
182. *UK HPR1000 - Assessment of the response to RO-UKHPR1000-0059 – Evidence of Production Excellence for the FirmSys platform,* Revision B, Revision 0, August 2021, ONR. 2021/62682
183. *RO Resolution Plan - RO-UKHPR1000-0059 - Control & Instrumentation - Evidence of Production Excellence for the FirmSys Platform,* Revision A, February 2021, CGN. [CM9 Ref. 2021/17076]
184. *Assessment Report of Production Excellence for FirmSys Platform,* GHX56100185GSNS44TR, Revision A, March 2021, CGN. [CM9 Ref. 2021/23924]
185. *Assessment Report of Production Excellence for FirmSys Platform,* GHX56100185GSNS44TR, Revision B, April 2021, CGN. [CM9 Ref. 2021/35018]
186. *IET Code of Practice: Competence for safety related systems practitioners,* 2016, The IET.
187. *Step 2 Assessment of the Control and Instrumentation of UK HPR1000 Reactor,* ONR-GDA-UKHPR1000-AR-18-001, Revision 0, October 2018, ONR. [CM9 Ref. 2018/236571]
188. *Assessment of the Response to RO-UKHPR1000-0001 - Diverse Actuation System Shortfalls,* ONR-NR-AN-20-027, Revision 0, March 2021, ONR. [CM9 Ref. 2021/22283]
189. *Safety Requirements of the KDS [DAS],* GHX06501002DIYK03GN, Revision E, November 2020, CGN. [CM9 Ref. 2020/316482]
190. *Simple Hardware Based Platform Technical Research Summary Report,* GHX56100022GSN44TR, Revision B, August 2019, CGN. [CM9 Ref. 2019/255649]
191. *Development Plan of Simple Hardware Based Platform,* GHX56100033GSNS44TR, Revision A, June 2020, CGN. [CM9 Ref. 2020/195739]
192. *Equipment Qualification Plan of Simple Hardware Based Platform,* GHX56100034GSNS44TR, Revision A, June 2020, CGN. [CM9 Ref. 2020/195746]
193. *Development Plan of Simple Hardware Based Platform,* GHX56100033GSNS44TR, Revision B, January 2021, CGN. [CM9 Ref. 2021/8290]
194. *Development Plan of Simple Hardware Based Platform,* GHX56100033GSNS44TR, Revision C, May 2021, CGN. [CM9 Ref. 2021/40266]
195. *Equipment Qualification Plan of Simple Hardware Based Platform,* GHX56100034GSNS44TR, Revision C, April 2021, CGN. [CM9 Ref. 2021/33278]
196. *Topic Report of HOLLiAS-N Platform,* GHX56100002GSNS44TR, July 2019, CGN. [CM9 Ref. 2019/227688]
197. *Topic Report of SpeedyHold Platform,* GHX5600003GNS44TR, Revision A, July 2019, CGN. [CM9 Ref. 2019/229997]
198. *Suitability Analysis Report of the Selected Platform Applicability to the KDA [SA I&C] System Requirements,* GHX56100066GSNS44TR, Revision A, May 2020, CGN. [CM9 Ref. 2020/159834]
199. *Product Excellence Summary Paper for Algorithm Calculation and Power Failure Protection Function of SpeedyHold,* GHX56100165GSNS44TR, Revision A, November 2020, CGN. [CM9 Ref. 2020/316503]
200. *Modification Form - Design Modification to Improve the Independence and Reliability of KDA [SA I&C],* M89-GHTCN000200, Revision A, April 2021, CGN. [CM9 Ref. 2021/30979]
201. *Step 4 Assessment of Cross-cutting Topics for the UK HPR1000 Reactor,* ONR-NR-AR-21-007, Revision 0, November 2021, ONR. [CM9 Ref. 2021/47905]

202. *Demonstration of Production Excellence for the RPS [PS],* GHX56100037GSNS44TR, Revision C, April 2021, CGN. [CM9 Ref. 2021/35837]
203. *Application Software Verification and Validation Plan of FirmSys Based I&C Systems,* GHX56100031GSNS44TR, Revision B, December 2020, CGN. [CM9 Ref. 2020/321765]
204. *Comparison of UK HPR1000 Protection System RPS [PS] with IEC 61513,* GHX00630002DIYK03GN, Revision A, August 2019, CGN. [CM9 Ref. 2019/251265]
205. *PComparison Analysis of Protection System (RPS [PS]) with IEC60880,* GHX56100041GSNS44TR, Revision A, September 2020, CGN. [CM9 Ref. 2020/286760]
206. *Comparison Analysis of FirmSys Based I&C Systems with IEC 60987,* GHX56100032GSNS44TR, Revision A, September 2020, CGN. [CM9 Ref. 2020/286790]
207. *Overtemperature T and Overpower T Protection Setpoints Design,* GHX00100002DRRG03GN, Revision F, March 2021, CGN. [CM9 Ref. 2021/26821]
208. *Production Excellence Sample for the RPS [PS] (RPS-SRS-0045),* GHX06002033DIYK03GN, Revision A, January 2021, CGN. [CM9 Ref. 2021/8469]
209. *Production Excellence Sample for the RPS [PS] (RPS-SRS-0285),* GHX56100182GSNS44TR, Revision A, January 2021, CGN. [CM9 Ref. 2021/8284]
210. *BSC of Protection System,* GHX06002002DIYK03GN, Revision C, June 2020, CGN. [CM9 Ref. 2020/196626]
211. *Strategy for Conducting ICBMs Activities for RPS [PS],* GHX06100015DIYK03GN, Revision C, January 2021, CGN. [CM9 Ref. 2021/6745]
212. *Design Specification of RPS [PS],* GHX56100018GSNS44TR, Revision D, February 2021, CGN. [CM9 Ref. 2021/12263]
213. *Analysis Report of the HVAC Sample Systems,* GHX08000010DCNT03TR, Revision C, May 2021, CGN. [CM9 Ref. 2021/43093]
214. *Equipment Qualification Plan of FirmSys Platform,* GHX56100005GSNS44TR, Revision A, April 2019, CGN. [CM9 Ref. 2019/124196]
215. *Report on Equioment Qualification Test for FirmSys Platform_Main Control,* GHX56100076GSNS44TR, Revision A, June 2020, CGN. [CM9 Ref. 2020/196633]
216. *RPS – Protection System Design Manual Chapter 6 System Operation and Maintenance,* GHX17RPS006DIYK45GN, Revision D, November 2020, CGN. [CM9 Ref. 2020/316593]
217. *Periodic Test Requirement of Protection System (PS),* GHX06002017DIYK03GN, Revision A, June 2019, CGN. [CM9 Ref. 2019/183964]
218. *Design Specification of Protection System RPS PS,* GHX56100018GSNS44TR, Revision E, June 2021, CGN. [CM9 Ref. 2021/51498]
219. *Design Specification of Safety Automation System (SAS),* GHX56100026GSNS44TR, Revision D, February 2021, CGN. [CM9 Ref. 2021/12202]
220. *Confinement Schedule,* GHX00600379DRAF02GN, Revision A, November 2020, CGN. [CM9 Ref. 2020/309769]
221. *Demonstration of Production Excellence for the SAS,* GHX56100038GSNS44TR, Revision C, April 2021, CGN. [CM9 Ref. 2021/35835]
222. *Strategy for Conducting ICBMs Activities for SAS,* GHX06100001DIYK03GN, Revision C, January 2021, CGN. [CM9 Ref. 2021/6744]
223. *Functional Requirements of the KDS [DAS],* GHX00600248DRAF02GN, Revision C, October 2020, CGN. [CM9 Ref. 2020/305435]
224. *KDS [DAS] System Requirements Specification,* GHX06002022DIYK03GN, Revision D, January 2021, CGN. [CM9 Ref. 2021/8313]

225. *Demonstration of Production Excellence for PSAS and KIC [PCICS],* GHX56100053GSNS44TR, Revision B, April 2021, CGN. [CM9 Ref. 2021/35833]
226. *Suitability Analysis Report of the Selected Platform Applicability to the PSAS & KIC [PCICS] System Requirements,* GHX56100065GSNS44TR, Revision A, May 2020, CGN. [CM9 Ref. 2020/159840]
227. *Comparison Analysis of PSAS and KIC [PCICS] with IEC 62138,* GHX56100044GSNS44TR, Revision A, October 2020, CGN. [CM9 Ref. 2020/303849]
228. *UKHPR1000 - Assessment of the response to RO-UKHPR1000-0057 – Independent Confidence Building Measures for complex systems,* Revision 0, August 2021, ONR. 2021/62679
229. *RO-UKHPR1000-0057 - C&I - Independent Confidence Building Measures for Complex Control and Instrumentation Systems - Final Resolution Plan,* RO-UKHPR1000-0057 - C&I - Independent Confidence Building Measures for Complex Control and Instrumentation Systems - Final Resolution Plan - Andrew White - 11 December 2020, Revision A, December 2020, CGN. [CM9 Ref. 2020/320176]
230. *Strategy for Conducting ICBMs Activities for PSAS and KIC [PCICS],* GHX06100021DIYK03GN, Revision C, January 2021, CGN. [CM9 Ref. 2021/6699]
231. *Strategy for Conductiong ICBMs Activities for KDA [SA I&C],* GHX06100020DIYK03GN, Revision C, January 2021, CGN. [CM9 Ref. 2021/6751]
232. *Feasibility Study Report for Static Analysis of Protection System.,* GHX06100010DIYK03GN, Revision A, November 2020, General Nuclear Systems Ltd. 2020/316490
233. *Feasibility Study Report for Source Code Comparison of Protection System.,* GHX06100011DIYK03GN, Revision A, November 2020, General Nuclear Systems Ltd.. 2020/316480
234. *Feasibility Study Report for Statistical Testing of Protection System,* GHX06100012DIYK03GN, Revision B, February 2021, CGN. [CM9 Ref. 2021/12201]
235. *Feasibility Study Report for Statistical Testing of Protection System,* GHX06100012DIYK03GN , Revision A, November 2020, CGN. [CM9 Ref. 2020/316488]
236. *NCSC Secure Design Principles,* Version 1.0, May 2019, NCSC. https://www.ncsc.gov.uk/collection/cyber-security-design-principles
237. *The CPA Build Standard,* Version 1.4, October 2018, NCSC. http://ncsc.gov.uk/files/CPA-Build_Standard_1-4.pdf
238. *Step 4 Security Assessment of the UK HPR1000 Reactor,* ONR-NR-AR-21-010, Revision 0, December 2021, ONR. [CM9 Ref. 2021/50021]
239. *Cyber Risk Assessment Methodology,* GDARECEDFSEC000007, Revision 0, June 2019, GNSL. [CM9 Ref. 2019/159487]
240. *Cyber Security Risk Assessment Methodology,* HPR-GDA-REPO-0108, Revision 1, February 2020, GNSL. [CM9 Ref. 2020/65561]
241. *Cyber Security Risk Assessment Report,* GDA-REC-GNSL-SEC-000026, Revision 1, August 2020, GNSL. [CM9 Ref. 2020/238146]
242. *Cyber Security Risk Assessment Report,* GDA-REC-GNSL-SEC-000026, Revision 2, January 2021, GNSL. [CM9 Ref. 2021/29846]
243. *Scope for UK HPR1000 GDA Project,* HPR-GDA-REPO-0007, Revision 1, July 2019, CGn. [CM9 Ref. 2019/209339]
244. *Cyber Security Design Requirements Specification,* HPR-GDA-SPEC-0114, Revision 0, December 2020, GNSL. [CM9 Ref. 2020/317676]
245. *Cyber Security Design Requirements Specification,* HPR-GDA-SPEC-0114, Revision 1, March 2021, GNSL. [CM9 Ref. 2021/21834]
246. *RPS Cyber Security Design Requirements Compliance Gap Analysis,* HPR-GDA-REPO-0159, Revision 0, March 2021, GNSL. [CM9 Ref. 2021/28187]

247. *PSAS Cyber Security Design Requirements Compliance Gap Analysis,* HPR-GDA-REPO-0158, Revision 0, April 2021, GNSL. [CM9 Ref. 2021/28707]
248. *RPS Cyber Security Design Requirements Compliance Gap Analysis,* HPR-GDA-REPO-0159, Revision 1, May 2021, GNSL. [CM9 Ref. 2021/39188]
249. *PSAS Cyber Security Design Requirements Compliance Gap Analysis,* HPR-GDA-REPO-0158, Revision 1, May 2021, GNSL. [CM9 Ref. 2021/39189]
250. *The Strategy for the Use of HMIs,* GHX06100012DIKX03GN, Rev C, January 2021, CGN. [CM9 Ref. 2021/8492]
251. *Overall Scheme for Control Room System,* Rev. E, May 2019, CGN. [CM9 Ref. 2019/156200]
252. *Assessment of the Response to RO-UKHPR1000-0052 - Design and Safety Case for Class 1 and 2 Human Machine Interfaces Employed in the Main Control Room and Remote Shutdown Station,* Revision 0, July 2021, ONR. [CM9 Ref. 2021/49566]
253. *Design Specification of Severe Accident System,* GHX56100028GSNS44TR, Revision D, March 2021, CGN. [CM9 Ref. 2021/27285]
254. *PS-SCID Requirements Specification,* Rev. A, January 2021, CGN. [CM9 Ref. 2021/270]
255. *SAS-SCID Requirements Specification,* Rev. A, January 2021, CGN. [CM9 Ref. 2021/278]
256. *Class 1 and Class 2 Hardwired Requirements Specification,* Rev. A, January 2021, CGN. [CM9 Ref. 2021/280]
257. *Class 1 and Class 2 Hardwired HMI Design Specification,* Rev. B, Febuary 2021, CGN. [CM9 Ref. 2021/12203]
258. *Optioneering Analysis Report for Class 1 Comupter-based HMI of RPS[PS],* Rev. A, January 2021, CGN. [CM9 Ref. 2021/276]
259. *Optioneering Analysis Report for Class 2 Computer-based HMI of SAS,* Rev. A, January 2021, CGN. [CM9 Ref. 2021/6757]
260. *Class 1 and 2 Hardwired HMI Design Specification,* GHX56100174GSNS44TR, Rev B, Febuary 2021, CGN. [CM9 Ref. 2021/12203]
261. *Analysis Report for Class 1 and Class 2 Hardwired HMI,* Rev. A, January 2021, CGN. [CM9 Ref. 2021/6742]
262. *Alarm Function and Alarm Processing Requirement Specification,* Rev. A, March 2020, CGN. [CM9 Ref. 2020/83025]
263. *Methodology of SMART Devices Substantiation,* GHX06002016DIYK03GN, Rev A, July 2019, CGN. [CM9 Ref. 2019/230007]
264. *Methodology of Smart Devices Substantiation,* GHX06002016DIYK03GN, Rev E, March 2021, CGN. [CM9 Ref. 2021/17862]
265. *Computer Based Safety Systems,* Revision 6, April 2019, ONR. [CM9 Ref. 2020/264582]
266. *Questionnaire for Smart Devices Assessment (F-SC1) Based on IEC Nuclear Standards,* GHX06002028DIYK03GN, Rev A, July 2020, CGN. [CM9 Ref. 2020/208158]
267. *Questionnaire for Smart Devices Assessment (F-SC2 and F-SC3) Based on IEC Nuclear Standards,* GHX06002029DIYK03GN, Rev C, Febuary 2021, CGN. [CM9 Ref. 2021/16892]
268. *Questionnaire for Smart Devices Assessment Based on IEC Industrial Standards,* GHX06002030DIYK03GN, Rev C, Febuary 2021, CGN. [CM9 Ref. 2021/16890]
269. *Summary Report for F-SC1 Smart Device Assessment Trial,* GHX06100016DIYK03GN, Rev C, March 2021, CGN. [CM9 Ref. 2021/17860]
270. *Assessment Table for F-SC1 Smart Device Trial,* GHX06100037DIYK03GN, Rev A, January 2021, CGN. [CM9 Ref. 2021/2332]

271. *UK HPR1000 Generic Design Assessment - Level 4 Control and Instrumentation Meeting to inspect evidence relating to the Class 1 smart deveice trial assessment,* ONR-NR-CR--20-955, Revision 0, February 2021, ONR. [CM9 Ref. 2021/14145]
272. *Summary Report for F-SC3 Smart Device Assessment Trial,* GHX06100035DIYK03GN, Rev C, March 2021, CGN. [CM9 Ref. 2021/17861]
273. *Assessment Table for F-SC3 Smart Device Trial,* GHX06100038DIYK03GN, Rev A, January 2021, CGN. [CM9 Ref. 2021/3078]
274. *UK HPR1000 Generic Design Assessment - Level 4 Control and Instrumentation Meeting,* ONR-NR-CR-20-942, Revisions 0, February 2021, ONR. [CM9 Ref. 2021/12586]
275. *Lessons Learnt from Smart Device Assessment Trial,* GHX06100039DIYK03GN, Rev A, January 2021, CGN. [CM9 Ref. 2021/8307]
276. *Pre-Construction Safety Report Chapter 33 ALARP Evaluation,* HPR/GDA/PCSR/0033, Revision 002, November 2021, GNSL. [CM9 Ref. 2021/85113]
277. *Guidance on the Demonstration of ALARP,* NS-TAST-GD-005, Revision 11, November 2020, ONR. https://www.onr.org.uk/operational/tech_asst_guides/index.htm

Annex 1

Relevant Safety/Security Assessment Principles Considered During the Assessment

SAP/SyAP No	SAP/SyAP Title	Description
MS.2	Leadership and management for Safety – Capable Organisation	The organisation should have the capability to secure and maintain the safety of its undertakings.
SC.4	The regulatory assessment of safety cases – Safety case characteristics	A safety case should be accurate, objective and demonstrably complete for its intended purpose.
SC.7	The regulatory assessment of safety cases – Safety case maintenance	A safety case should be actively maintained throughout each of the lifecycle stages, and reviewed regularly.
EKP.2	Engineering principles: key Principles – Fault tolerance	The sensitivity of the facility to potential faults should be minimised.
EKP.3	Engineering principles: key Principles – 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.
ECS.1	Engineering principles: safety classification and standards – Safety categorisation	The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be identified and then categorised based on their significance with regard to safety.
ECS.2	Engineering principles: safety classification and standards – 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	Engineering principles: safety classification and standards – 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.5	Engineering principles: safety classification and standards – Use of experience, tests or analysis	In the absence of applicable or relevant codes and standards, the results of experience, tests, analysis, or a combination thereof, should

SAP/SyAP No	SAP/SyAP Title	Description
		be applied to demonstrate that the structure, system or component will perform its safety function(s) to a level commensurate with its classification.
EQU.1	Engineering principles: equipment qualification – 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	Engineering principles: design for reliability – 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	Engineering principles: design for reliability – Redundancy, diversity and segregation	Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components.
EDR.3	Engineering principles: design for reliability – 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	Engineering principles: design for reliability – 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	Engineering principles: reliability claims – Form of claims	The reliability claimed for any structure, system or component should take into account its novelty, experience relevant to its proposed environment, and uncertainties in operating and fault conditions, physical data and design methods.
ERL.2	Engineering principles: reliability claims – Measures to achieve reliability	The measures whereby the claimed reliability of systems and components will be achieved in practice should be stated.

SAP/SyAP No	SAP/SyAP Title	Description
ERL.3	Engineering principles: reliability claims – Engineered safety measures	Where reliable and rapid protective action is required, automatically initiated, engineered safety measures should be provided.
ECM.1	Engineering principles: commissioning – Commission testing	Before operating any facility or process that may affect safety it should be subject to commissioning tests defined in the safety case.
EMT.1	Engineering principles: maintenance, inspection and testing – 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	Engineering principles: maintenance, inspection and testing - Frequency	Structures, systems and components should receive regular and systematic examination, inspection, maintenance and testing as defined in the safety case.
EMT.5	Engineering principles: maintenance, inspection and testing - Procedures	Commissioning and in-service inspection and test procedures should be adopted that ensure initial and continuing quality and reliability.
EMT.6	Engineering principles: maintenance, inspection and testing – 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	Engineering principles: maintenance, inspection and testing – 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	Engineering principles: maintenance, inspection and testing – 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	Engineering principles: ageing and degradation – 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	Engineering principles: ageing and degradation – 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.

SAP/SyAP No	SAP/SyAP Title	Description
ELO.4	Engineering principles: layout - 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.
ESS.1	Engineering principles: safety systems – 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	Engineering principles: safety systems – 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	Engineering principles: safety systems – 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.4	Engineering principles: safety systems – Adequacy of initiating variables	The variables used to initiate a safety system action should be identified and shown to be suitable and sufficient for the system to achieve its safety function(s).
ESS.5	Engineering principles: safety systems – 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.7	Engineering principles: safety systems – 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	Engineering principles: safety systems – 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	Engineering principles: safety systems – Definition of capability	The capability of a safety system, and of each of its constituent sub-systems and components, should be defined and substantiated.

SAP/SyAP No	SAP/SyAP Title	Description
ESS.11	Engineering principles: safety systems – 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	Engineering principles: safety systems – 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.15	Engineering principles: safety systems – 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.
ESS.17	Engineering principles: safety systems – Faults originating from safety systems	Potential faults originating from within safety systems (e.g. due to spurious or mal-operation) should be identified and protection against them provided.
ESS.18	Engineering principles: safety systems – Failure independence	No design basis event should disable a safety system.
ESS.19	Engineering principles: safety systems – Dedication to a single task	A safety system should be dedicated solely to the provision of its allocated safety functions.
ESS.20	Engineering principles: safety systems – Avoidance of connection 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	Engineering principles: safety systems – 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	Engineering principles: safety systems – 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	Engineering principles: safety systems – Allowance for unavailability of equipment	In determining the safety systems to be provided, allowance should be made for the potential unavailability of equipment.

SAP/SyAP No	SAP/SyAP Title	Description
ESS.25	Engineering principles: safety systems – Taking safety systems out of service	The vetoing or the taking out of service of any safety system function should be avoided.
ESS.26	Engineering principles: safety systems – Maintenance and testing	Maintenance and testing of a safety system should not initiate a fault sequence.
ESS.27	Engineering principles: safety systems – 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	Engineering principles: control and instrumentation of safety-related systems – provision of 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.5	Engineering principles: control and instrumentation of safety-related systems – Standards for equipment in safety-relates 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	Engineering principles: control and instrumentation of safety-related systems – 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.
ESR.7	Engineering principles: control and instrumentation of safety-related systems – Communication 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.
SyDP 7.1	FSyP 7 - Cyber Security and Information Assurance – Effective Cyber and Information Risk Management	Dutyholders should maintain arrangements to ensure that CS&IA risk is managed effectively.

SAP/SyAP No	SAP/SyAP Title	Description
SyDP 7.2	FSyP 7 - Cyber Security and Information Assurance – Information security	Dutyholders should maintain the confidentiality, integrity and availability of sensitive nuclear information and associated assets.
SyDP 7.3	FSyP 7 - Cyber Security and Information Assurance – Protection of Nuclear Technology and Operations	Dutyholders should ensure their operational and information technology is secure and resilient to cyber threats by integrating security into design, implementation, operation and maintenance activities.
SyDP 7.4	FSyP 7 - Cyber Security and Information Assurance – Physical Protection of Information	Dutyholders should adopt appropriate physical protection measures to ensure that information and associated assets are protected against a wide range of threats.
SyDP 7.5	FSyP 7 - Cyber Security and Information Assurance – Preparation for and Response to Cyber Security Incidents	Dutyholders should implement well-tested plans, policies and procedures to reduce their vulnerability to cyber security incidents (especially from the most serious threats of terrorism or cyber-attack), non-malicious leaks and other disruptive challenges.

Annex 2

Assessment Findings

Note: These Assessment Findings must be read in the context of the sections of the report listed in this table, where further detail is provided regarding the matters that led to the findings being raised.

Number	Assessment Finding	Report Section
AF-UKHPR1000-0024	The licensee shall complete a compliance demonstration of the detailed design of all UK HPR1000 C&I systems important to safety, against the requirements of IEC 61513 and its normative standards. The demonstration should consider all aspects of the design lifecycle, including the processes that govern how the design is developed, and the results should inform the safety case. For any areas of non-compliance the licensee shall implement reasonably practicable measures to address the shortfalls.	4.2.1 4.6.2.1
AF-UKHPR1000-0026	The licensee shall demonstrate that the hardware reliability of the detailed design of the UK HPR1000 C&I systems fulfils the requirements derived from the safety analysis. The hardware reliability analyses should follow a methodology that is informed by international standards and relevant good practice. The analyses should give particular consideration to the following as a minimum: ▪ clear definition and justification of the boundaries of the analyses, including any assumptions and constraints; ▪ the identification of hazards, such as those caused by internal failures or faults, their consequences on system operation, and the measures to control these; and ▪ the identification of all factors that may affect reliability, including self-supervision capabilities, requirements for proof testing and maintenance.	4.3.1 4.6.2.1

Number	Assessment Finding	Report Section
AF-UKHPR1000-0027	The licensee shall demonstrate that the detailed designs for the diverse Component Interface Module and Signal Pre-processing Module provide resilience to common cause failures and shall develop the detailed designs for those modules in accordance with the concept designs provided in GDA, or equivalent alternatives.	4.3.1
AF-UKHPR1000-0029	The licensee shall, as part of detailed design of all UK HPR1000 C&I systems important to safety, determine whether additional measures to provide separation and segregation to protect against consequential effects caused by internal and external plant hazards are reasonably practicable. The analysis should include, but not be limited to, the following: ▪ separation and segregation of sensors located in 'exception to segregation' areas; ▪ separation and segregation of C&I cabinets associated with different systems; ▪ separation and segregation of cable routes for different systems within the same division; and ▪ control measures to reduce the risk of electromagnetic interference and radio frequency interference induced faults.	4.3.1
AF-UKHPR1000-0030	The licensee shall develop and justify examination, maintenance, inspection and testing arrangements for the UK HPR1000 C&I systems important to safety that reflect the safety case requirements, detailed design of the systems, and licensee choices for test intervals. This should include demonstration that the system architectures are suitable to support the maintenance and testing strategy.	4.4.1

Number	Assessment Finding	Report Section
AF-UKHPR1000-0031	The licensee shall develop production excellence evidence for the detailed design of the FirmSys platform, to justify that FirmSys is suitable to form the basis of the UK HPR1000 Reactor Protection System and Safety Automation System. This shall comprise, as a minimum, the following activities, or equivalent: ▪ define the scope of production excellence evidence necessary to support the safety case, and how this will be presented in a way that facilitates independent oversight; ▪ consideration of the safety objectives of the platforms and systems, and the need to implement measures to control the effects on system operation of internal failures and faults; ▪ revisit the self-assessment and compensating strategy developed during GDA, demonstrating that all of the gaps in the FirmSys platform have been identified, along with means to address those gaps; ▪ validate the schedule developed in GDA, including any changes necessary to resolve this finding, making allowance for enhanced regulatory oversight to be provided; and ▪ demonstrate that the organisational capability and capacity required for development of the FirmSys platform for the UK HPR1000, including that required to maintain independent oversight, can be maintained throughout the programme of work.	4.5.1.1

Number	Assessment Finding	Report Section
AF-UKHPR1000-0033	The licensee shall demonstrate the production excellence of the HOLLiAS-N and SpeedyHold platforms for the UK HPR1000, using an equivalent methodology to that applied to the Class 1 FirmSys platform during GDA. This shall give particular consideration to the following, as a minimum: ▪ the identified safety objectives of the platform and systems; ▪ the need to implement measures to control the effects on system operation of internal failures and faults; and ▪ the validity and appropriateness of the claims, including those related to testing and test coverage.	4.5.3.1
AF-UKHPR1000-0034	The licensee shall establish a mechanism by which the requirements for UK HPR1000 C&I platforms and systems can be unambiguously and completely established and managed, and that this can be demonstrated to be so, ensuring that: ▪ all functional and non-functional requirements are defined; ▪ the source of each individual requirement is identified; ▪ requirements contain only one concept or actionable element; ▪ requirements can be unambiguously traced both forwards and backwards through the design and safety case documentation; ▪ requirements are complete, unambiguous and consistently documented; ▪ assumptions and constraints are clearly and unambiguously documented; and ▪ the potential for errors in the manipulation, translation and use of requirements is minimised.	4.6.1.1 4.6.2.1 4.6.3.1 4.6.4.1 4.6.5.1 4.6.6.1 4.9.1

Number	Assessment Finding	Report Section
AF-UKHPR1000-0035	The licensee shall demonstrate the production excellence of the detailed design of the UK HPR1000 computer-based C&I systems important to safety, using an equivalent methodology to that applied to the Class 1 FirmSys platform during GDA. This shall give particular consideration to the following as a minimum: ▪ the identified safety objectives of the platform and systems; ▪ the need to implement measures to control the effects on system operation of internal failures and faults; and ▪ all reactor operating modes for which the systems are required to act.	4.6.1.1 4.6.2.1 4.6.4.1 4.6.5.1 4.6.6.1
AF-UKHPR1000-0036	The licensee shall demonstrate that the risks arising from misconfiguration of the Reactor Protection System and Safety Automation System through use of the software maintenance tool are reduced so far as is reasonably practicable, by: ▪ identifying the hazards arising from the connection and operation of the Reactor Protection System and Safety Automation System maintenance tool, including, but not limited to, inadvertent connection, incorrect use, faults and cyber threats; ▪ identifying measures to control these hazards, considering a hierarchy of controls; and ▪ demonstrating that the controls are effective and reliable.	4.6.1.1
AF-UKHPR1000-0037	The licensee shall demonstrate that the frequency of spurious actuation of the UKHPR1000 C&I systems important to safety is minimised as low as reasonably practicable, considering: ▪ the architectural arrangement; ▪ the potential for faults to occur due to hardware failures; ▪ the potential for errors to occur in digital communications; and ▪ the potential for common cause software failures to occur.	4.6.1.1

Number	Assessment Finding	Report Section
AF-UKHPR1000-0038	The licensee shall demonstrate that hardwired inputs to the Safety Automation System from lower safety classified systems cannot compromise delivery of the Safety Automation System safety functions.	4.6.2.1
AF-UKHPR1000-0040	The licensee shall, during detailed design of the Diverse Actuation System, demonstrate that all reasonably practicable measures have been taken to ensure that the system fails safely on loss of power.	4.6.3.1
AF-UKHPR1000-0041	The licensee shall ensure that relevant standards are applied to the detailed design of the Plant Standard Automation System, including hardware standards, and a demonstration is provided that the design approach is commensurate to the required reliability and integrity.	4.6.4.1
AF-UKHPR1000-0042	The licensee shall assess the nuclear safety risks arising from incorrect operation of the Plant Computer Information and Control System impacting the Rod Position Indication and Rod Control System, and implement any reasonably practicable measures required to control those risks.	4.6.5.1
AF-UKHPR1000-0043	The licensee shall demonstrate that the programmable hardware-based Component Interface Module can be exhaustively tested and that all risks associated with the design are reduced so far as is reasonably practicable.	4.7.1
AF-UKHPR1000-0044	The licensee shall, for all systems which contain third party software, implement a strategy for independent confidence building measures which, together with production excellence, allows risk control to be demonstrated.	4.7.1
AF-UKHPR1000-0045	The licensee shall, as part of detailed design of the C&I systems, develop the cyber security risk assessment to include all C&I systems important to safety, and all interfaces between and within those systems. The assessment should follow a methodology that is at least as rigorous as that developed for GDA, and should include demonstration that measures are in place to address all identified vulnerabilities.	4.8.1

Number	Assessment Finding	Report Section
AF-UKHPR1000-0046	The licensee shall resolve the residual cyber security vulnerabilities identified in the GDA cyber security risk assessment report as part of detailed design. This should include the potential modifications proposed during GDA.	4.8.1
AF-UKHPR1000-0047	The licensee shall complete cyber security compliance analysis for all computer-based C&I systems important to safety and implement measures to address all instances of partial or non-compliance.	4.8.1
AF-UKHPR1000-0048	The licensee shall implement independent security assurance measures for the UK HPR1000 C&I systems important to safety. These should address, as a minimum, the following: ▪ measures to provide confidence that adequate security arrangements have been put in place by equipment suppliers to minimise security risks impacting C&I system development; ▪ measures to provide confidence that security design risks impacting the safety performance of C&I systems are mitigated; ▪ a graded approach to the levels of rigour and independence required for assurance measures that is informed by the safety and security significance of the system; ▪ assurance that security has been considered throughout the development lifecycle of systems; ▪ definition of the activities to be undertaken including objectives, inputs, outputs, methods and success criteria; and ▪ the organisational capability and capacity required to undertake independent assurance activities. The independent security assurance programme should be in accordance with the strategy submitted in GDA, or an equivalent alternative.	4.8.1

Number	Assessment Finding	Report Section
AF-UKHPR1000-0049	The licensee shall justify the permissive functions on UK HPR1000 C&I systems important to safety. The justification shall consider all permissive signals and should as a minimum address the following: ▪ the potential consequences of the failure of the Protection System Safety Control and Instrumentation Device to act when required in all operating modes; ▪ the potential consequences of the spurious actuation of the Protection System Safety Control and Instrumentation Device in all operating modes; ▪ the justification for holding the plant in a specific mode of operation whilst awaiting reinstatement of the Protection System Safety Control and Instrumentation Device; ▪ the potential for permissive signals to compromise diversity in detection of faults; ▪ the suitability of the categorisation of the permissive functions ▪ the holistic effects on plant operating procedures; and ▪ the risks associated with single and common cause failures.	4.9.1
AF-UKHPR1000-0051	The licensee shall develop and demonstrate the adequacy of a process for the identification and justification of smart devices. This process should address the following as a minimum: ▪ the responsibilities for the identification and justification of smart devices, including in packaged plant; ▪ the specification of requirements for the use and justification of smart devices; ▪ the organisational capacity and the skills and experience required for smart device assessors) and intelligent customers for smart device justifications; and ▪ the provision of key points in the process that would allow for decisions to be made as to whether continuation of the justification is warranted.	4.10.1

Number	Assessment Finding	Report Section
AF-UKHPR1000-0052	The licensee shall, as the detailed design develops, review and update the C&I safety case to ensure that: ▪ claims and arguments that are dependent on evidence that will be produced in site-specific stages are demonstrated to be met by that evidence; ▪ gaps in the underpinning evidence are highlighted and resolved; ▪ evidence is consistently referenced and that there is bi-directional traceability through claims, arguments and evidence and across related areas of the safety case; ▪ evidence demonstrably supports the claims and arguments against which it is claimed; and ▪ references to evidential documents are to the latest versions. ▪	4.2.1 4.6.1 4.6.2 4.11.1