Office for Nuclear Regulation

New Reactor Division – Generic Design Assessment

Step 2 Assessment of the Control and Instrumentation of UK HPR1000 Reactor

Assessment Report ONR-GDA-UKHPR1000-AR-18-001
Revision 0
October 2018

Published 10/18

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

EXECUTIVE SUMMARY

This report presents the results of my Control and Instrumentation (C&I) assessment of the UK HPR1000 undertaken as part of Step 2 of the Office for Nuclear Regulation's (ONR) Generic Design Assessment (GDA).

The GDA process calls for a step-wise assessment of the Requesting Party's (RP) safety submission with the assessments increasing in detail as the project progresses. Step 2 of GDA is an overview of the acceptability, in accordance with the regulatory regime of Great Britain, of the design fundamentals, including ONR's review of key nuclear safety and nuclear security claims (or assertions). The aim is to identify any fundamental safety or security shortfalls that could prevent ONR from permitting the construction of a power station based on the design.

During GDA Step 2 my work has focused on the assessment of the C&I aspects within the UK HPR1000 Preliminary Safety Report (PSR), and a number of supporting references and supplementary documents submitted by the RP, focusing on design concepts and claims.

The standards I have used to judge the adequacy of the RP's submissions in the area of C&I have been primarily ONR's Safety Assessment Principles (SAPs), in particular SAPs EDR.3, EDR.4, ECS.2 and the ESS series, and also ONR's Technical Assessment Guides (TAGs). I have also made use other relevant standards and guidance, particularly IAEA SSG-30, IEC61513 and IEC61226.

My GDA Step 2 assessment work has involved regular engagement with the RP in the form of technical exchange workshops and progress meetings, including meetings with the plant designers.

The UK HPR1000 PSR is primarily based on the Reference Design, Fangchenggang Unit 3 (FCG3), which is currently under construction in China. Key aspects of the UK HPR1000 preliminary safety case related to C&I, as presented in the PSR, its supporting references and the supplementary documents submitted by the RP, can be summarised as follows:

- The FCG3 C&I architecture consists of multiple interconnected C&I systems which are classified based upon their nuclear safety significance within the FCG3 plant.
- C&I systems are provided to ensure effective reactivity control, heat removal and confinement of radioactive material.
- Reactor protection is performed by a dedicated Reactor Protection System which is categorised as being of the highest safety classification, and this system is backed up by a Diverse Actuation System of lower safety classification.
- Reactor control under normal operating conditions is performed by a control system which is of a different design and which is claimed to act independently from those systems performing reactor protection functions.

During my GDA Step 2 assessment of the UK HPR1000 aspects of the safety case related to C&I I have identified a number of areas of strength, including the following:

- The C&I systems are designed to provide five independent levels of defence in depth covering normal operation, accident mitigation, diverse accident mitigation, severe accidents and emergency response – this approach aligns with established UK relevant good practice regarding defence-in-depth.
- The Reactor Protection System has been allocated the highest level of safety classification and contains multiple levels of equipment redundancy, being of a four-train design, and in this regard reflects UK relevant good practice.

During my GDA Step 2 assessment of the UK HPR1000 aspects of the safety case related to C&I, I have identified the following significant areas that require follow-up:

- The contents of the PSR addressing C&I design was based upon the design of a reactor currently under construction in China (FCG3) and a safety case based upon the UK design is to be provided later in GDA. In Steps 3 and 4 of GDA I will assess (against UK Relevant Good Practice) any significant differences between the UK design and the FCG3 design which were not considered within my Step 2 assessment.
- I raised a Regulatory Observation (RO) concerning shortfalls in the design of the Diverse Actuation System. In response, the RP produced an RO resolution plan which I judged to be credible and timely; I will review the RP's implementation of this plan later in the GDA process. The planned RO closure date is August 2019.
- The RP's safety case contained claims concerning the ability of the C&I equipment to support the overall station safety case, covering functional performance, reliability and design substantiation, but arguments and evidence to support these claims were not available for assessment within Step 2; I will assess these aspects later in the GDA process.
- The ability of C&I architecture to withstand potential Common Cause Failures is a key aspect of the design, and as more safety case information becomes available I will consider this area in greater detail later in the GDA process.

During my GDA assessment of the Step 2 safety case, I have not identified any fundamental safety shortfalls in the area of C&I that should prevent the issue of a Design Acceptance Confirmation (DAC) for the UK HPR1000 design.

LIST OF ABBREVIATIONS

ALARP	As Low As Reasonably Practicable
BMS	Business Management System
BSO	Basic Safety Objective (in SAPs)
C&I	Control and Instrumentation
CAE	Claims, Arguments and Evidence
CGN	China General Nuclear Power Corporation
CINIF	C&I Nuclear Industry Forum
DAC	Design Acceptance Confirmation
DAS[KDS]	Diverse Actuation System
EA	Environment Agency
EDF	Électricité de France
FCG3	Fangchenggang Unit 3 design (HPR1000)
F-SCn	FCG3 safety classification (n = 1, 2, or 3)
GNI	General Nuclear International
GNS	Generic Nuclear System Ltd
GSR	Generic Security Report
FS	Fault Studies
HF	Human Factors
HMI	Human Machine Interface
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
JPO	(Regulators') Joint Programme Office
KDA[SAI&C])	Severe Accident I&C system
KDS[DAS]	Diverse Actuation System
NAEMES	Nuclear Accident Emergency Management System
NPP	Nuclear Power Plant
ONR	Office for Nuclear Regulation

PAMS	Post-Accident Monitoring System
PCER	Pre-construction Environmental Report
PCSR	Pre-construction Safety Report
PFD	Probability of Failure on Demand
PIE	Postulated Initiating Event
PSA	Probabilistic Safety Assessment
PSAS	Plant Standard Automation System
PSR	Preliminary Safety Report (includes security and environment)
RGP	Relevant Good Practice
RHWG	Reactor Harmonization Working Group (of WENRA)
RI	Regulatory Issue
RIA	Regulatory Issue Action
RO	Regulatory Observation
ROA	Regulatory Observation Action
RP	Requesting Party
RQ	Regulatory Query
SAP(s)	Safety Assessment Principle(s)
SAS	Safety Automation System
SFAIRP	So far as is reasonably practicable
TAG	Technical Assessment Guide(s)
TSC	Technical Support Contractor
TSF	Technical Support Framework
WENRA	Western European Nuclear Regulators' Association

TABLE OF CONTENTS

Tables

1 INTRODUCTION

1. The Office for Nuclear Regulation's (ONR) Generic Design Assessment (GDA) process calls for a step-wise assessment of the Requesting Party's (RP) safety submission with the assessments increasing in detail as the project progresses. General Nuclear System Ltd (GNS) has been established to act on behalf of the three joint requesting parties (China General Nuclear Power Corporation (CGN), Électricité de France (EDF) and General Nuclear International (GNI)) to implement the GDA of the UK HPR1000 reactor. For practical purposes GNS is referred to as the 'UK HPR1000 GDA Requesting Party'.

2. During Step 1 of GDA, which is the preparatory part of the design assessment process, the RP established its project management and technical teams and made arrangements for the GDA of the UK HPR1000 reactor. Also, during Step 1 the RP prepared submissions to be assessed by ONR and the Environment Agency (EA) during Step 2.

3. Step 2 commenced in November 2017. Step 2 of GDA is an overview of the acceptability, in accordance with the regulatory regime of Great Britain, of the design fundamentals, including ONR's assessment of key nuclear safety and nuclear security claims (or assertions). The aim is to identify any fundamental safety or security shortfalls that could prevent ONR permitting the construction of a power station based on the design.

4. My assessment has followed my GDA Step 2 Assessment Plan for Control and Instrumentation (Ref. 1) prepared in October 2017 and shared with GNS to maximise openness and transparency.

5. This report presents the results of my C&I assessment of the UK HPR1000 as presented in the UK HPR1000 Preliminary Safety Report (PSR) Chapter 8 'Instrumentation and Control' (Ref. 2) and relevant supporting documentation (Refs 3 to 8). A full list of submissions is provided in the UK HPR1000 Document Submittal list (Ref. 9).

2 ASSESSMENT STRATEGY

6. This section presents my strategy for the GDA Step 2 assessment of the C&I aspects of the UK HPR1000. It also includes the scope of the assessment and the standards and criteria I have applied.

2.1 Scope of the Step 2 Control and Instrumentation Assessment

7. The objective of my GDA Step 2 assessment was to assess relevant design concepts and claims made by the RP related to C&I. In particular, my assessment has focussed on the following:

- structure of the safety case – Claims, Arguments and Evidence (CAE)
- C&I architecture
- key C&I systems
- probabilistic claims for C&I systems
- categorisation and classification
- application of ALARP principles

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

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

- Reviewed the RP's GDA scope in relation to C&I
- Discussed with the RP their intentions regarding submissions for Step 3
- Discussed with the RP their proposals for the contents and scope of Chapter 8 of the Pre-Construction Safety Report (PCSR).

2.2 Standards and Criteria

10. For ONR, the primary goal of the GDA Step 2 assessment is to reach an independent and informed judgment on the adequacy of a preliminary nuclear safety and security case for the reactor technology being assessed. Assessment was undertaken in accordance with the requirements of the Office for Nuclear Regulation (ONR) How2 Business Management System (BMS) guide NS-PER-GD-014 (Ref. 10).

11. In addition, the Safety Assessment Principles (SAPs) (Ref. 11) constitute the regulatory principles against which duty holders' and RPs' safety cases are judged. Consequently the SAPs are the basis for ONR's nuclear safety assessment and have therefore been used for the GDA Step 2 assessment of the UK HPR1000. The SAPs 2014 Edition is aligned with relevant International Atomic Energy Agency (IAEA) and International Electrotechnical (IEC) standards and guidance for C&I.

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

13. The relevant SAPs, IAEA standards, IEC standards and WENRA reference levels are embodied and expanded on in the Technical Assessment Guides (TAGs) on C&I (Ref. 12). These guides provide the principal means for assessing the C&I aspects in practice

2.2.1 Safety Assessment Principles

14. The key SAPs (Ref. 11) which informed my assessment were SAPs EKP, ECS, EQU, EDR, ERL, ECM, EMT, EAD, ELO, EHA, ESS, ESR, EES and ECV (see Table 1 for further details).

2.2.2 Technical Assessment Guides

15. The following key Technical Assessment Guides have been used to inform my assessment (Ref. 12):

- NS-TAST-GD-003 'Safety Systems'
- NS-TAST-GD-005 'Demonstration of ALARP'
- NS-TAST-GD-031 'Safety Related Instrumentation'
- NS-TAST-GD-046 'Computer Based Safety Systems'
- NS-TAST-GD-094 'Categorisation of Safety Functions and Classification of Structures, Systems and Components'

2.2.3 National and International Standards and Guidance

16. The following national and international standards and guidance have been considered as part of this assessment:

- Relevant IAEA standards (Ref. 13)
  - Safety Classification of Structures, Systems and Components in Nuclear Power Plants, International Atomic Energy Agency (IAEA), Specific Safety Guide SSG-30
  - Design of Instrumentation and Control Systems for Nuclear Power Plants, International Atomic Energy Agency (IAEA), Specific Safety Guide SSG-39
- WENRA references (Ref. 14)
  - WENRA Reactor Safety Reference Levels (January 2007)
- Other international standards (Ref. 15)
  - IEC 61508 - Functional safety of electrical/electronic/programmable electronic safety-related systems (parent standard for the design of E/E/PE safety-related systems)
  - IEC 61513 - Nuclear power plants — Instrumentation and control important to safety — General requirements for systems
  - IEC 61226 - Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions

2.3 Use of Technical Support Contractors

17. During Step 2 I have engaged a Technical Support Contractors (TSC) to support the following specific aspects of my assessment of the C&I for the UK HPR1000:

- Adequacy of C&I overall systems architecture design

18. The TSC has provided technical advice and has supported my assessment, working under my close direction and supervision. A record of the TSC assessment is provided in Ref. 16.

19. I have been able to use the analysis provided by the TSC to provide evidence to support a number of the RQs which I raised.

20. I have reviewed the TSC's conclusions as stated in the TSC report (Ref. 16) and I am content that they clearly support my conclusions regarding the adequacy of the Step 2 C&I safety case as documented within section 5. Within the TSC report the TSC identified at total of twenty potential shortfalls, termed Technical Observations (TOs). Eleven of the TOs have been directly addressed by RP responses to RO/RQs and by items identified for follow-up within this report, and the remainder have been deferred for further consideration during Step 3 (see Altran Technical Note documenting TO reconciliation (Ref. 17)).

21. It should be noted that the regulatory judgement on the adequacy of the C&I preliminary safety case for the UK HPR1000 has been made exclusively by ONR.

2.4 Integration with Other Assessment Topics

22. Early in GDA, I recognised the importance of working closely with other inspectors (including Environment Agency's inspectors) as part of the C&I assessment process. Similarly, other inspectors sought input from my assessment of the C&I for the UK HPR1000. I consider these interactions are key to the success of the project in order to prevent or mitigate any gaps, duplications or inconsistencies in ONR's assessment. From the start of the project, I have endeavoured to identify potential interactions between the C&I and other technical areas, with the understanding that this position will evolve throughout the UK HPR1000 GDA.

23. The key interactions I have identified are:

- Fault Studies (FS): this discipline determines the nuclear safety significance of functions assigned to Structures and Components (SSC), including C&I systems important to safety. Interactions with the RP on the development of the fault studies analysis have commenced during GDA Step 2 and are being led by the Fault Studies inspector.

- Probabilistic Safety Assessment (PSA): provides input into the determination of the reliability claims assigned to C&I systems. This interaction has commenced during GDA Step 2 and is being led by the PSA inspector.

- Human Factors (HF): In relation to C&I, HF determines the adequacy of the design of interfaces provided to enable operators to interact with the plant through C&I systems. HF also informs the allocation of safety functions between the human and C&I systems. The overall assessment of the adequacy of the HF facilities is being led by the HF lead inspector in coordination with myself.

- Electrical Engineering: This discipline considers the adequacy of the safety case for the electrical systems which provide electrical power to C&I systems important to safety, under normal operating conditions and under fault conditions. This work is being led by the Electrical inspector in coordination with myself.

24. In addition to the above, during GDA Step 2 there have been interactions between other technical assessment areas and myself, including Mechanical Engineering,

Management of Safety and Quality assurance (MSQA) and Internal Hazards. Although these interactions have been of an informal nature, they help to ensure that ONR maintains a consistent assessment approach across assessment disciplines. Such informal interactions are expected to continue through GDA Steps 3 and 4.

3 REQUESTING PARTY'S SAFETY CASE

26. During Step 2 of GDA the RP submitted a PSR and other supporting references, which outline a preliminary nuclear safety and security case for the UK HPR1000. This section presents a summary of the RP's preliminary safety case in the area of C&I. It also identifies the documents submitted by the RP which have formed the basis of my C&I assessment of the UK HPR1000 during GDA Step 2.

3.1 Summary of the RP's Preliminary Safety Case in the Area of C&I

27. The aspects covered by the UK HPR1000 preliminary safety case in the area of C&I can be broadly grouped under the subject headings of the following six subsections:

3.1.1 Claims, Arguments and Evidence (CAE)

28. ONR GDA guidance (Ref. 19) states that ONR will focus on assessing RP Claims in Step 2, Arguments in Step 3 and Evidence in Step 4. In order to facilitate a meaningful GDA assessment it is important that the RP's fully developed GDA safety case presents a clear and structured definition of the Claims, Arguments and Evidence (CAE) relevant to C&I, and that the C&I CAE are consistent with the overall plant CAE and also with the relevant CAE made for associated disciplines (e.g. PSA, FS and HF).

29. It is stated within the PSR that the UK HPR1000 I&C will be designed based on the C&I design of FCG3, also that the GDA design for the UK has not been declared and that consequently no detailed UK HPR1000 design information was provided. The PSR states that its purpose is to '*provide confidence that the I&C systems to be developed for UK HPR1000 will be able to demonstrate compliance with UK regulatory requirements'*. Given this statement, I assumed for the purpose of my Step 2 assessment that broadly any safety claims provided for the FCG3 design within the Step 2 safety case were directly applicable to the UK HPR1000 design.

30. The safety case was not fully organised into a Claims, Arguments and Evidence structure, however three explicit claims were provided in section 8.2 of the PSR which gives a general commitment to comply with relevant standards and to provide the necessary safety functions (see section 4.1 for more detail). In addition, the PSR together with supporting documents (see section 3.2) contain many explicit and implicit claims concerning the adequacy of the C&I design within FCG3. These claims may be broadly grouped under the following subject headings:

- C&I architecture
- C&I systems
- probabilistic claims for C&I
- Categorisation and Classification
- ALARP

31. These headings are considered in the following sub-sections.

3.1.2 Control and Instrumentation Architecture

32. The PSR Chapter 8 (Ref. 2) contained a number of general safety claims for the FCG3 C&I architecture design covering aspects such as functional coverage, Single Failure Criteria (SFC), Defence in Depth (DiD), independence, physical separation and redundancy. At my request, additional C&I architectural information was provided in two further supporting documents:

- Supplement to PSR Chapter 8 for HPR1000 (FCG3) Instrumentation & Control Overall Architecture Description (Ref. 4)

- Comparison of HPR1000 (FCG3) Instrumentation and Control Overall Architecture Design With IEC61513 (Ref. 5)

33. The first of these documents contained additional information concerning C&I architectural design features, and the second provided an analysis of the design of the architecture against relevant requirements of international standard IEC 61513 (Ref. 15).

3.1.3 C&I Systems

34. PSR Chapter 8 identifies and describes those C&I systems within the FCG3 design which were identified as being important to nuclear safety. The RP allocates the highest safety classification (F-SC1) to the Reactor Protection Systems (RPS) and the second highest (F-SC2) to the Safety Automation System (SAS) in recognition of the key safety functions performed by these systems (note; see section 3.1.5 for information concerning C&I classification). The RP allocates a lower safety classification (F-SC3) to the remaining systems due to their claimed lower safety significance. Further detail concerning FCG3 C&I systems is provided in section 4.1.3 of this report.

3.1.4 Probabilistic Claims for C&I Systems

35. My initial review of the RP safety case within Chapter 8 of the PSR (Ref. 2) did not identify any probabilistic claims for C&I systems. I brought this issue to the attention of the RP and emphasised ONR's expectation that all high-level safety claims should be available in Step 2. In response the RP provided the document 'Safety Claims for Numerical Targets Made on the I&C Systems for HPR1000 (FCG3)' (Ref. 6). I assessed this document as described in section 4.1.4.

3.1.5 Classification and Categorisation of Systems, Structures and Components

36. Chapter 4 of the PSR (Ref. 3) provides a number of high level claims concerning the RP's approach to Classification and Categorisation, and defines three levels of safety function categorisation FC1, FC2 and FC3. It is also stated that the class of SSCs that fulfil specific safety functions should be consistent with the category of that safety function. Three safety classes are defined which correspond to the three safety functions, namely F-SC1, F-SC2 and F-SC3.

37. The RP also provided the supporting reference 'Methodology of Safety Categorisation and Classification' (Ref. 7). Within the document it was states that its purpose is to present the UK HPR1000 safety function categorisation and System, Structure and Component (SSC) classification methodology, and to justify that it was suitable for the UK context, in support of GDA and future site licensing.

38. This document provides an overview of the RP's approach to categorisation and classification, and provides a description of how this approach aligns with IAEA and UK terminology.

39. A key claim within this document is that the UK HPR1000 methodology applied to SSCs, including C&I systems, was based on international Relevant Good Practice (RGP).

3.1.6 ALARP

40. The RP provided a submission 'ALARP Methodology' (Ref. 8). In this document the RP states that it was recognised that 'there is a fundamental requirement for the

Requesting Party to set out their process to reduce risk to a level that is As Low As Reasonably Practicable (ALARP)'.

41. This document states that the RP's ALARP approach includes consideration of four areas in the demonstration of ALARP:

a) Comparison with Relevant Good Practice (RGP)

b) Identification and evaluation of options (Optioneering)

c) Risk assessment, as a way of understanding the significance of the issue to the overall demonstration of ALARP

d) Implementation of reasonably practicable improvements

42. It also states that the safety case for the UK HPR1000 will (following further development) summarise the major modifications implemented within the UK HPR1000 design, including the associated optioneering, and provide justification (of the claim) that no further reasonably practicable improvements are available.

43. In addition, section 8.2 of the PSR states that the three claims provided within that section, covering C&I high level claims for safety functional coverage and standards compliance, 'demonstrated' that the FCG3 C&I design 'supports the As Low As Reasonably Practicable (ALARP) targets'.

3.2 Basis of Assessment: RP's Documentation

44. The RP's information that formed the basis for my GDA Step 2 assessment of the safety claims related to the C&I aspects of the UK HPR1000 is presented in the following primary reference:

- Preliminary Safety Report (PSR) - Chapter 8 Instrumentation and Control (Ref. 2)

45. The information in this primary reference was supplemented by information provided in the following supporting references:

- Supplement to PSR Chapter 8 for HPR1000 (FCG3) Instrumentation & Control Overall Architecture Description (Ref. 4)
- Comparison of HPR1000 (FCG3) Instrumentation and Control Overall Architecture Design With IEC61513 (Ref.5)
- Safety Claims for Numerical Targets Made on the I&C Systems for HPR1000 (FCG3) (Ref.6)

46. In addition, during April 2018 the RP submitted to ONR, for information, an advance copy of the UK HPR1000 Pre-Construction Safety Report (PCSR) Chapter 8 (Ref. 18) which addresses C&I aspects of the design. Having early visibility of the scope and content of this chapter/s has been useful in the planning and preparation of my GDA Step 3 assessment work.

4 ONR ASSESSMENT

47. This assessment has been carried out in accordance with HOW2 guide NS-PER-GD-014, “Purpose and Scope of Permissioning” (Ref. 10).

48. My Step 2 assessment work has involved continuous engagement with the RP’s C&I specialists, including one Technical Exchange Workshop (in China), and five main progress meetings (in UK).

49. During my GDA Step 2 assessment, I have identified some gaps in the documentation formally submitted to ONR. Consistent with ONR’s Guidance to Requesting Parties (Ref. 19), these normally lead to Regulatory Queries (RQs) being issued. At the time of writing, I have raised 14 RQs to facilitate my C&I Step 2 assessment (Ref. 20).

50. Similarly, and again consistent with ONR’s Guidance to Requesting Parties (Ref. 19), more significant shortfalls against regulatory expectations in the generic safety case are captured by issuing Regulatory Observations (ROs). I have raised one RO, which described in section 4.3:

- RO-UKHPR1000-0001- Diverse Actuation System (DAS) Design Shortfalls

51. Details of my GDA Step 2 assessment of the UK HPR1000 preliminary safety case in the area of C&I, including the conclusions I have reached, are presented in the following sub-sections of this report. This includes the areas of strength I have identified, as well as significant items that require follow-up during subsequent Steps of the GDA of UK HPR1000.

4.1 Claims, Arguments and Evidence (CAE)

4.1.1 Assessment

52. I based my Step 2 assessment of this aspect of the Step 2 C&I safety case on the expectations set out in ONR GDA guidance (Ref. 19) which emphasised the need for a clear trail from claims, through the arguments, to the evidence that fully supports the safety case conclusions.

53. This claims-arguments-evidence (CAE) approach is commonly used in structuring safety cases in the nuclear industry and elsewhere. ONR sees advantages in this structured approach being employed within C&I safety cases. The guidance also states that the aim within GDA Step 2 safety assessments is to assess the key claims and identify any fundamental safety shortfalls that could prevent ONR permitting reactor construction.

54. ONR applies a goal-setting regulatory regime, is not prescriptive about the form or structure of safety cases provided for regulatory assessment and does not mandate the use of a CAE structure. However during my Step 1 and Step 2 engagements with the RP I have discussed the advantages of adopting a CAE structure for the C&I safety case.

55. My Step 2 assessment plan (Ref. 1) identified that a key aim of my assessment was to perform a review of the RP’s safety submission/s to confirm whether the claims related to C&I that underpin the safety of the UK HPR1000 were sufficient to enable Step 3 assessment to commence. My initial review of Chapter 8 of the PSR revealed that three explicit claims are made – see below. The Step 2 safety case also contains embedded within it many of the high level additional claims/assertions which I would expect such a C&I safety case to contain, e.g. covering DiD, diversity,

categorisation/classification (my assessment of the adequacy of such claims is reported in sections 4.2 to 4.6 of this report).

56. The three explicit claims for C&I contained within the PSR, are as follows:

- The HPR1000 (FCG3) C&I design scheme satisfies the requirements in related codes and standards. It also satisfies the safety requirements and function requirements of HPR1000 (FCG3) power plant.
- The C&I platforms and equipment adopted in HPR1000 (FCG3) meet related I&C function requirements.
- The C&I systems support the SSCs in performing their required duties, and enable the detection of potentially dangerous faults or conditions to allow appropriate safety actions.

57. I raised RQ-UKHPR1000-0042 (Ref. 20) in which I queried the basis for these claims. In response the RP confirmed that the current CAE mode was not structured to provide clear linkage with other PSR chapters such as FS and PSA, but steps were being taken to address this shortfall. The RP also stated that their intention was to provide five high level C&I claims in a revised CAE safety case, as follows:

i) The safety functional requirements have been derived for the (C&I) systems

ii) The system design (of each system) satisfies the safety functional requirements

iii) All reasonably practical measures have been adopted to improve the design of the (C&I) systems

iv) The system performance (of each C&I system) will be validated by commissioning and testing

v) The effects of ageing of each system have been addressed in the design

4.1.2 Strengths

58. I identified no particular areas of strength within the RP's Step 2 safety case regarding the application of a Claims, Arguments and Evidence approach, although I acknowledge that the RP has indicated that it will improve this moving forward in GDA.

4.1.3 Items that Require Follow-up

59. During my GDA Step 2 assessment of the Claims, Arguments and Evidence aspect of the C&I safety case I have identified the following additional potential shortfalls that I will follow-up during Step 3 of GDA:

- In response to RQ-UKHPR1000-0042 the RP describes how a revised approach to the use of CAE within the safety case, specifically an improved Claims structure, is under development. The alignment of this revised approach with ONR expectations and assessment of the safety case substantiation of the revised C&I claims will be assessed during Step 3 (for example to assess the capability of C&I systems to meet the assigned UK HPR1000 functional safety requirements)
- The CAE addressing C&I design were based upon the design of a reactor currently under construction in China (FCG3) and a safety case based upon the

UK HPR1000 design is to be provided later in GDA. In Steps 3 and 4 of GDA I will assess any identified significant differences between the CAE for the UK design and the FCG3 design which were not considered within this Step 2 assessment

60. During my GDA Step 2 assessment of Claims, Arguments and Evidence I have identified the following area that may require research to be undertaken by the RP in order to underpin the safety claims in C&I. I will follow-up this matter, as appropriate, during Step 3:

- The application of a CAE-based/goal-based approach to C&I safety cases. This is an area of on-going UK research under the auspices of the UK C&I Nuclear Safety Forum (CINIF). With my encouragement, the RP is investigating the option of joining this forum as an active member. Membership would enable the RP to influence the direction of on-going and future research projects, and would also provide access to the results of completed research.

4.1.4 Conclusions

61. In arriving at my conclusions concerning the use of Claims, Arguments and Evidence within the Step 2 safety case I have taken the following matters into account:

- the contents of the C&I chapter within the PSR is based upon design information for FCG3, and UK-specific information will be provided later in GDA;

- although the C&I chapter in the PSR did not address probabilistic claims, a supplemental document has been provided which provided high level claims concerning probabilistic claims for C&I systems important to safety (see section 4.4); and

- the RP's response to RQ-UKHPR1000-0042 describes how an improved strategy concerning the application of a CAE approach, specifically an improved Claims structure, is under development.

62. I have therefore concluded that, although the current version of the safety case as documented in PSR Chapter 8 does not demonstrate the application of a consistent and effective application of a CAE approach, the RP has provided sufficient additional information to give me sufficient confidence that this aspect of the safety case will be improved later in the GDA process.

4.2 Control and Instrumentation Architecture

4.2.1 Assessment

63. My Step 2 C&I assessment included consideration of the adequacy of the design of the C&I architecture, i.e. the overall design of the C&I, consisting of the C&I systems important to safety and their interconnections. This approach was consistent with the strategy set out in my Step 2 C&I assessment plan (Ref. 1).

64. I based my initial assessment on the contents of Chapter 8 of the PSR (Ref. 2). I used the ONR SAPs ESS (Safety Systems) and ESR (Control and instrumentation of safety-related systems) to inform my assessment and judgement of the adequacy of the RP's safety case. ONR's TAGs covering Safety Systems (NS-TAST-GD-003) and Computer Based Safety Systems (NS-TAST-GD-046) along with international standards IEC 61513, "Nuclear power plants Instrumentation and control important to safety General requirements for systems" (Ref. 15), and IEC 61508, "Functional safety

of electrical/electronic/programmable electronic safety-related systems" (Ref. 15) also informed my judgement. Table 1 of this report, covering applicable SAPs, gives additional information concerning SAPs which I used to inform my assessment.

65. Chapter 8 of the PSR contained an overview of the C&I architecture but I found that the level of detail provided was insufficient to support a meaningful Step 2 assessment. I therefore requested additional information, particularly regarding the various data paths used to transfer data between systems. In response the RP provided the report 'Supplement to PSR Chapter 8 for HPR1000 (FCG3) Instrumentation & Control Overall Architecture Description (Ref. 4). This document considerably enhanced my understanding of the C&I architecture but I found some of the text within this document ambiguous, and I subsequently raised RQ-UKHPR1000-0043 (Ref. 20). In response, the RP provided additional clarification (Ref. 20) which enabled me to complete my assessment.

66. I also identified a referenced document within the Step 2 safety case which could potentially further improve my understanding of the basis of the C&I architecture design and I raised RQ-UKHPR1000-0118 (Ref. 20) to request that this document be provided (late in the Step 2 assessment process). This additional document has not yet been received, but I consider that in broad terms sufficient information has been made available within other Step 2 safety case documents to enable a meaningful Step 2 assessment to be completed.

67. I considered the adequacy of the C&I architecture from a number of perspectives, which are summarised under the following headings.

Compliance with International RGP

68. The key international standard which is recognised by ONR as establishing many of the principles of UK RGP regarding C&I architecture is IEC61513 (Ref. 15). At my request, and to enable a meaningful Step 2 assessment to be performed, the RP provided an additional supporting reference 'Comparison of HPR1000 (FCG3) Instrumentation and Control Overall Architecture Design With IEC61513' (Ref. 5). I reviewed the first draft of this document and raised RQ-UKHPR1000-0006 (Ref. 20) as I had identified some additional information that could be provided to support my assessment. The supporting reference document was subsequently revised to provide this information (i.e. the requirements of section 5.4 of IEC61513 were added).

69. The revised document (Ref.5) set out the RP's high-level case for general compliance of the FCG3 C&I architecture with IEC61513. The following 'differences' between the FCG3 design and this international standard were identified by the RP:

    i) A signal transmission path existed from a lower classified system to a higher classified system – which was non-compliant with IEC61513 (Note: also see SAP ECS.2). I raised a number of RQs on this issue (see under heading 'Separation' below).

    ii) Use of development tools has not yet been addressed in the safety submissions received to date. I did not consider this issue to warrant a shortfall at this stage of GDA as I will be considering use of tools as a matter of course within GDA Steps 3 and 4. The point concerning tool use was also noted within the report produced by the ONR TSC as a Technical Observation type 1 (see Ref. 16 and section 2.3).

    iii) Assignment of safety functions to C&I for the UK HPR1000 design has yet to be performed. ONR has accepted that the safety case is being developed progressively and the RP has indicated that a Fault Schedule will be provided

post completion of ONR Step 2 assessment (please refer to Step 2 Summary Report (Ref.23) fault studies section for further detail if required). C&I functional assignment to C&I systems will be considered in GDA Steps 3 and 4.

iv) A Common Cause Failure (CCF) analysis methodology has not yet been defined and is under development. However, I did not consider the fact that a methodology was not yet available to be a hindrance to my completion of a meaningful Step 2 assessment. The methodology will be assessed under GDA Steps 3 and 4. Please note that I have raised a number RQs concerning C&I resilience to CCF (see under heading CCF/DiD below) and I identify resilience to CCF as a follow-up issue in section 4.2.3.

Separation

70. In order that faults do not propagate across system boundaries it is important that there is adequate functional separation between systems and adequate physical separation between the components which comprise the individual systems.

71. Regarding functional separation, my review of the Step 2 safety case documentation did identify a number of concerns, as documented in the following RQs:

72. RQ-UKHPR1000-0072 (Ref. 20) in combinations with RQ-UKHPR1000-0086 (Ref. 20) concerned data flows from a lower (Plant Computer Information and Control System) to a higher class system (a Safety Control and Information Device) - such data flows could potentially compromise the integrity of the higher class system. The information provided in response to these RQs established that this data flow was provided to more easily enable operators to perform control functions on Class 1 nuclear safety plant. The RP has stated that, if the integrity of this facility cannot be substantiated by the RP, then the facility could be safely disabled (by removing connecting cables). I considered that this information was sufficient to support my GDA Step 2 assessment. I will consider this issue in greater detail as more safety case information becomes available within Step 3.

73. RQ-UKHPR1000-0103 (Ref. 20) concerned the potential for flows of information over hardwired links connecting lower class systems to higher class systems to compromise resilience to CCF. In summary, the RP's response stated that such links were binary or analogue signals electrical signals with separation/segregation being provided through electrical isolation. The RP's response also identified that further information would be provided post-Step 2. I considered this response to be in line with my expectations and to be adequate for GDA Step 2. I will be considering this issue further as more information becomes available within Step 3.

74. RQ-UKHPR1000-0104 (Ref. 20) concerned the flow of data from lower class systems to higher class systems over digital networks which could compromise resilience to CCF. In response the RP confirmed that a number of data links were uni-directional and provided additional information which provided me with sufficient confidence in the RP's strategy for maintaining data integrity to support my Step 2 assessment (see section 4.2.3 'Items that require follow-up').

75. RQ-UKHPR1000-0128 (Ref. 20) concerning the potential for the integrity of data flowing from Class 1 equipment to be compromised through transmittal through equipment of a lower class. In response the RP stated that in non-fault conditions data flows may be through lower classified systems, but in fault conditions a Class 1 qualified route would be used. I could not determine from this response if under all circumstances Class 1 equipment would used for nuclear safety Category 1 functions, and I raised a follow up RQ – RQ-UKHPR1000-0149 (at time of writing there has been insufficient time to allow the RP to provide a response to this RQ). I considered the

response provided to RQ-UKHPR1000-0128 (Ref. 20) did progress my understanding of this aspect of the design and I will consider this issue in greater depth during my Step 3 assessment.

76. My assessment of the adequacy of physical separation consisted of a high-level review of the Step 2 C&I safety case documentation (see also entry against ELO.1 in Table 1). I noted that there was some evidence of physical separation between equipment providing different levels of DiD, e.g. three physically separated locations containing HMI facilities were to be provided – the Main Control Room, the Remote Shutdown Station and the Technical Support Centre. I did not identify any significant shortfalls, but this issue will be considered in greater depth in GDA Step 3.

Common Cause Failure/Defence in Depth (CCF/DiD)

77. The C&I systems are described in Chapter 8 of the PSR (Ref. 2) as providing five independent levels of defence in depth covering normal operation, accident mitigation, diverse accident mitigation, severe accidents and emergency response. I concluded that this approach was generally consistent with UK RGP, however I noted a number of potential shortfalls concerning CCF/DiD, and raised two RQs in this area (note: RO-UKHPR1000-001 is also relevant to this issue, see section 4.3 for further detail).

78. RQ-UKHPR1000-0117 (Ref. 20) concerning the extent of diversity between the prevention line and main defence line given that the equipment implementing these different lines were implemented using software/microprocessor technology and they were manufactured by different suppliers and used different equipment platforms. The issue of diversity is important as this is a key factor providing resilience to CCF. The RP also stated that a report addressing the extent of diversity between the equipment in these lines of defence would be produced in Step 3. I judged this response to be sufficient at this stage of GDA and I will consider the resilience of C&I to CCF in greater depth in Step 3.

79. RQ-UKHPR1000-0121 (Ref. 20) concerning the potential for the design of the Component Interface Module (CIM) to be a potential source of CCF affecting multiple layers of DiD. The role of the CIM is to prioritise actuation signals from multiple systems (e.g. the RPS, DAS and PSAS) to ensure that the system with the highest safety significance takes priority, so failure of this component has the potential to affect the functional performance of many systems. In response the RP stated that this issue has been identified as a gap against UK RGP and the RP has proposed to prepare a preliminary design for a revised CIM by December 2019. I considered this response to be adequate for this stage of GDA and I will consider the RP's response in Step 3.

Functional Coverage

80. ONR have acknowledged that functional requirements analysis for the UK design has not yet been completed by the RP, however my assessment of the Step 2 safety case did raise a number of concerns in this area, and I raised the following RQs:

81. RQ-UKHPR1000-0119 (Ref. 20) queried how the design would prioritise between manual and automatic control actions. The RP response provided me with adequate confidence that the relevance of this issue with respect to nuclear safety was recognised by the RP and that this issue was being systematically considered within the design process for the UK HPR1000, and I identified no shortfalls with respect to the high-level information provided. I will consider this issue in greater detail during GDA Step 3.

82. RQ-UKHPR1000-0120 (Ref. 20) concerned the extent of HMI provisions in the Remote Shutdown Station (RSS). The RP's response clarified that only a subset of equipment

would be provided at this facility compared to the full suite of facilities provided in the Main Control Room (MCR). It was not possible within Step 2 to determine if the proposed facilities within the RSS would be adequate for all UK HPR1000 fault scenarios (as a full analysis of UK HPR1000 Design Basis faults has yet to be presented by the RP) but, this is an issue that will be considered by ONR during GDA Step 3. I co-ordinated with the HF ONR lead to ensure that he was fully aware of my interactions with the RP in this area. I was content that the RP's response to this RQ was adequate to support my Step 2 assessment.

4.2.2 Strengths

83. The following areas of strength within the RP's Step 2 safety case are worthy of note:

- The C&I systems were claimed to provide five independent levels of defence in depth covering normal operation, accident mitigation, diverse accident mitigation, severe accidents and emergency response – this approach generally aligned with established UK relevant good practice. The five levels are summarised below:

  Level 1 – prevention line: PSAS
  Level 2 – main defence line: RPS + SAS
  Level 3 – diverse defence line: DAS
  Level 4 – severe accident defence line: SA I&C
  Level 5 – emergency response line: NAEMES

4.2.3 Items that Require Follow-up

84. During my GDA Step 2 assessment of C&I Architecture I have identified the following specific shortfalls:

- Diverse Actuation System design shortfalls (RO-UKHPR1000-0001); see section 4.3 for my detailed assessment of this issue.

85. During my GDA Step 2 assessment of C&I I have identified the following additional potential shortfalls that I will follow-up during Step 3 of GDA:

- C&I architecture resilience to CCF - I raised a number of Step 2 RQs concerning the potential vulnerability of the C&I architecture to CCF, and although I judged that the responses received were adequate to support entry into GDA Step 3, the safety case in this area was not fully developed, e.g. see the RP response to RQ-UKHPR1000-0121 (Ref. 20), and RQ-UKHPR1000-0149 (Ref. 20). (Note: the RP has committed to produce a CCF analysis in response to RQ-UKHPR1000-0117 which I will consider in Step 3).

- I identified an issue concerning data flows from a lower class to a higher class system, as documented in RQ-UKHPR1000-0086 and as discussed under 'Separation' above, which I will follow up later in the GDA process.

4.2.4 Conclusions

86. In arriving at my conclusions concerning the outcome of my Step 2 assessment of the adequacy of the C&I architecture design within the Step 2 safety case, I have taken the following matters into account:

- The information within the PSR covering C&I (Ref.2) is based upon design information for FCG3, and UK-specific information will be provided later in GDA.

- The information provided in the RP's Step 2 safety case documents (see section 3.2) was supplemented through the provision of additional documents (e.g. Ref. 4) and by the responses provided to RO-UKHPR1000-0001 and C&I RQs (as summarised within this report).

87. Taking these matters into account, and based on the outcome of my Step 2 assessment of C&I architecture, I have concluded that the RP has provided sufficient information enabling me to perform a meaningful Step 2 C&I assessment. I have not identified any fundamental safety shortfalls in this area, although I have identified a number of important topics to follow-up in GDA Step 3.

4.3 C&I Systems

4.3.1 Assessment

88. I identified the following C&I systems within the Step 2 safety case as being important to nuclear safety:

- Reactor Protection System (RPS)
- Safety Automation System (SAS)
- Plant Standard Automation System (PSAS)
- Diverse Actuation System (KDS[DAS])
- Post-Accident Monitoring System (PAMS)
- Severe Accident I&C System (KDA[SAI&C])
- Human Machine Interface (HMI)
- Nuclear Accident Emergency Management System [NAEMS]

89. In accordance with my Step 2 assessment plan (Ref. 1) I performed a high level sample-based assessment of the adequacy of those systems within the architecture which I considered to be of the highest safety significance, namely the RPS, SAS and the KDS[DAS]. My assessment is summarised below.

Reactor Protection System (RPS)

90. The classification of this system met my expectations in that it was assigned the highest level (F-SC1) of C&I safety classification within the FCG3 classification methodology.

91. The architecture of this system also met my expectations in that a 4 train design is proposed with two-out-of-four (2oo4) voting to be used to initiate a reactor trip. The use of a 4-train design provides resilience to system faults and provides redundancy to permit maintenance while the plant is operational. The fact that the 4-train design approach has been successfully used within UK operational PWR plant and within other new reactor designs which have successfully completed GDA (i.e. achieving Design Acceptance Confirmation (DAC) status) increased my confidence in the robustness of this proposed design.

92. The implementation technology proposed for the RPS is microprocessor/software-based. The fact that this technology has been licensed within the UK to implement

similar Class 1 high-integrity nuclear C&I systems increased my confidence in this aspect of the design. However, the safety cases for such systems have made extensive use of evidence supporting 'Production Excellence' and the implementation of 'Confidence-Building Measures' (see ESS.27 in Table 1 and NS-TAST-GD-046 (Ref. 12) for further information regarding UK RGP in this area). This is an aspect of the RP's C&I safety case which has yet to be developed, but which is not required to complete a meaningful Step 2 assessment. I will consider the detailed safety case later in the GDA process.

Safety Automation System (SAS)

93. The SAS was described within the safety case as performing the processing functions (automatic and manual control) and monitoring functions required to bring the reactor from a controlled state to a safe shutdown state, e.g. following a reactor trip initiated by the RPS. Within the FCG3 design this equipment was allocated to a safety class of lesser safety significance to the RPS (F-SC2), but of higher safety significance than that allocated to the Plant Standard Automation System (PSAS). My high-level Step 2 assessment did not reveal any non-compliance against UK RGP with regard to this classification approach, but I will be considering the RP's classification process in greater depth later within the GDA process.

94. The C&I platform to be used to implement this system was the same at that proposed for the RPS. However, as the SAS and the RPS were in the same 'level' of the five levels of protection (level 2) within the C&I architecture design (see section 4.2.2), I judged that the use of the same technology for the SAS and RPS should not introduce a vulnerability in regard to C&I DiD resilience to CCF across DiD levels, but I will consider this issue in more detail in Step 3.

95. The safety case claimed that this system would meet the single-failure-criteria (see SAP EDR. 4 in Table 1), which met my expectations.

96. The arguments and evidence to be provided by the RP in GDA Steps 3 and 4 will enable a more detailed assessment of the adequacy of this system to be performed, and I am content that sufficient Step 2 information was provided to enable me to perform a meaningful Step 2 assessment.

Diverse Actuation System (KDS[DAS])

97. The design proposed within the RP's safety case had the following features:

- The DAS was classified as being of low nuclear safety significance and allocated a classification of F-SC3 (which I judged to be generally equivalent to Class 3 within IEC61513 (Ref. 15) - which ONR recognises as establishing the basis of UK RGP).
- The system was not designed to meet the single failure criteria.
- The implementation platform was based on complex hardware technology.

98. I did not consider that the design as proposed met UK RGP as set out in relevant ONR guidance and in relevant international standards. I therefore raised RO-UKHPR1000-0001- Diverse Actuation System (DAS) Design Shortfalls (Ref. 21) to document my concerns. Within this Regulatory Observation (RO) I identified three significant shortfalls (please refer to the text within the RO for full details):

- Classification of the DAS – the classification was low and did not reflect the nuclear safety significance of this system and did not comply with RGP,
- Single Failure Criteria – I was concerned that this system could be rendered in-operational through the failure of a single component.

- The implementation platform was based upon the use of complex programmable components – I was concerned that the use of complex technology in the DAS, the RPS and in the PSAS could introduce vulnerability to CCF (e.g. due to latent design errors in complex components, due to cyber vulnerabilities, etc.).

99. In response, the RP produced a regulatory observation resolution plan (Ref. 22). I was content that the plan presented a credible and timely programme of work to address my concerns. The first deliverable identified in the plan is report 'Safety Requirements of the KDS [DAS]', due for delivery December 2018. The second and final delivery is report 'Simple Hardware Based Platform technical research summary report', due for delivery March 2019. The planned closure date for the RO is August 2019 (within GDA Step 3).

4.3.2 Strengths

100. The following areas of strength within the RP's Step 2 safety case for C&I systems are worthy of note within this report:

- The 4-train C&I architecture of the Reactor Protection System aligns with international and UK RGP.

- The RP has clearly acknowledged that the current design of the Diverse Actuation System has significant shortfalls against UK RGP and has set in place a credible plan to address these shortfalls.

4.3.3 Items that Require Follow-up

101. During my GDA Step 2 assessment of the adequacy of C&I systems important to safety I have identified the following specific shortfalls:

- Diverse Actuation System design shortfalls (RO-UKHPR1000-0001)

102. During Step 2 I did not consider the RP's approach to the substantiation of SMART instruments (i.e. instruments containing complex implementation technology), although my assessment identified that the design does contain such devices. The substantiation of SMART instruments has been challenging for UK licensees and RPs as a thorough and systematic approach is required in order to produce adequate CAE to justify their use in nuclear safety applications. Although not considered in Step 2, this is an aspect of the RP's safety case that I will consider later in the GDA process.

4.3.4 Conclusions

103. Based on the outcome of my Step 2 assessment of C&I Systems I was content that the Step 2 safety case contained sufficient information to support my Step 2 assessment of this aspect of the design. I performed a high-level review of three of the most safety significant C&I systems and concluded that two of these (RPS and SAS) were generally in line with my expectations. I identified significant concerns regarding the design of the third system (DAS), however I am content that the RP has put in place a credible plan to address these concerns within the resolution plan to RO-UKHPR1000-0001 (Ref. 21).

4.4 Probabilistic Claims for C&I Systems

4.4.1 Assessment

104. My initial review of the RP safety case within Chapter 8 of the PSR (Ref. 2) did not identify any probabilistic claims for the C&I systems. At my request, the RP provided the following supplemental safety case document:

- Safety Claims for Numerical Targets Made on the I&C Systems for HPR1000 (FCG3) (Ref. 6)

105. This document allocated target probability of failure on demand (pfd) reliability claims to C&I systems important to safety as follows:

- RPS - $1x10^{-4}$ pfd
- SAS - $1x10^{-2}$ pfd
- KDS[DAS] - $1x10^{-1}$ pfd

The underlying analysis to justify that these claims were adequate to support the overall UK HPR1000 safety case was not made available during Step 2.

106. I found that these claimed reliability figures to be broadly aligned with claims that have previously been substantiated for similar systems within the UK although there is a need for further information on, for example, safety functional allocation, likely effects of CCF, independence arguments, etc. I will confirm my judgement on whether these claims are within the recommended bounding limits set out in ONR guidance (e.g. SAP ESS.27 and NS-TAST-GD-046) in Step 3.

4.4.2 Strengths

107. I have not identified any specific strengths regarding C&I probabilistic claims.

4.4.3 Items that Require Follow-up

108. During my GDA Step 2 assessment of C&I probabilistic claims I have identified the following potential shortfall that I will follow-up during Step 3 of GDA:

- The underlying analysis to link the probabilistic C&I claims to the overall plant safety case was not available during GDA Step 2; assessment of this aspect of the safety case will be performed when this information becomes available later in GDA. Areas of future interest in the follow-up assessment will include; alignment of C&I reliability claims with the plant safety case; alignment with ONR SAP Numerical Targets (Ref. 11), alignment with ONR guidance (e.g. NS-TAST-GD-046 (Ref. 12)) and compatibility of C&I reliability claims with the safety case estimates for Postulated Initiating Events (PIE) due to C&I spurious outputs.

4.4.4 Conclusions

109. Based on the outcome of my Step 2 assessment of probabilistic claims for C&I systems, I have concluded that the claims made for the RPS, SAS and KDS[DAS] systems are broadly consistent with UK RGP as set out in ONR SAPs and guidance documents, and with previously substantiated claims for similar systems licensed within the UK. However, the analysis underlying these claims has yet to be completed by the RP. Therefore I have concluded that there remains a significant risk that the RP's eventual claims in this area (to be submitted post-Step 2) may not be consistent with UK RGP.

4.5 Categorisation of Safety Functions and Classification of Structures, Systems and Components

4.5.1 Assessment

110. My assessment in this area has focused on the RP's approach to the classification of C&I systems. I have assessed Chapter 8 of PSR (Ref. 2) and I have reviewed the supporting "Methodology of Safety Categorisation and Classification" (Ref. 7) document. Please note that Classification of safety functions was considered within the FS assessment (the Step 2 Summary Report (Ref. 23) contains an overview of the FS assessment).

I used the ONR SAPs ECS.1 (Safety categorisation), ECS.2 (Safety classification of structures, systems and components) to inform my assessment. ONR's Categorisation and Classification NS-TAST-GD-094 (Ref. 12) has also been used to support my judgements together with IEC 61226 (Ref. 15) and the IAEA Specific Safety Guide SSG-30 (Ref. 5).

111. The PSR described how three levels of C&I classification had been used within the FCG3 design;

- F-SC1 (highest)
- F-SC2 (intermediate)
- F-SC3 (lowest)

112. The safety case also listed standards relevant to C&I equipment of different classifications, e.g. IEC60880 was proposed for F-SC1software development and IEC62138 was proposed for F-SC2 software development. The standards identified against each level of classification were generally in line with my expectations and provided confidence that this aspect of the UK-specific safety case (to be fully developed by the RP later in the GDA process) will align with the general principles of UK RGP.

4.5.2 Strengths

113. The RP has outlined a categorisation and classification methodology where the most nuclear safety significant C&I equipment is assigned to the highest nuclear safety class, and this general approach aligns with UK RGP.

4.5.3 Items that Require Follow-up

114. I did not identify any specific shortfalls regarding FCG3 C&I classification and categorisation to follow up, but I will consider this aspect of the UK HPR1000 safety case as more information becomes available later in the GDA process. I will be using the following guidance to inform my assessment - ONR SAPs ECS.1, ECS.2, NS-TAST-GD-094 (Ref. 12), IEC61513 (Ref.15), IEC 61226 (Ref. 15) and the IAEA Specific Safety Guide SSG-30 (Ref. 13).

4.5.4 Conclusions

115. Based on the outcome of my Step 2 assessment, I have concluded that the Step 2 safety case provided sufficient confidence regarding the high-level alignment of the RP's C&I classification methodology with C&I UK RGP to complete a meaningful Step 2 assessment. I identified no significant shortfalls. Please refer to the ONR Summary Report (Ref. 23) for ONR's conclusions regarding the RP's overall approach to SSC Categorisation and Classification.

4.6 ALARP Considerations

4.6.1 Assessment

116. ONR guidance document 'Demonstration of ALARP' NS-TAST-GD-005 (Ref. 12) states that a nuclear licensee has a legal requirement to reduce risks so far as is reasonably practicable (SFAIRP). The concept of SFAIRP is normally expressed in terms of reducing risks to "As Low As Reasonably Practicable" (ALARP), the terms SFAIRP and ALARP being synonymous in ONR guidance documents.

117. Within the ONR GDA Step 2 assessment project, ALARP was defined as a 'Cross Cutting' issue, i.e. an issue which had implications across many disciplines and which justified consideration within the ONR GDA process in its own right. This issue was addressed within the GDA Step 2 UK HPR1000 Summary Report (Ref. 23).

118. As described in section 3.1.6, the RP's approach to ALARP is addressed by an ALARP methodology document (Ref. 8). This document describes a process where gaps against relevant good practice are identified and then a defined process followed to determine what, if any, design changes would be made to the reference design to arrive at a UK HPR1000 design which demonstrably reduced risks ALARP.

119. The C&I design presented by the RP for assessment under GDA Step 2 is defined within Chapter 8 of the PSR; this design was not supported by a UK HPR1000 C&I ALARP analysis. However, I am content that the general application of ALARP to the C&I design will be addressed by the RP later in the GDA process. Assessment of C&I ALARP will be co-ordinated with the overall ONR assessment of this cross cutting matter.

120. Within Step 2 I raised Regulatory Observation RO-UKHPR1000-0001(Ref. 20) which identified a number of shortfalls (i.e. gaps) against RGP in the design of the DAS. I will be considering the RP's application of ALARP principles to address these shortfalls in GDA Steps 3 and 4.

4.6.2 Strengths

121. I have not identified any particular strengths regarding ALARP for C&I.

4.6.3 Items that Require Follow-up

122. During my GDA Step 2 assessment of ALARP I have identified the following specific shortfalls relating to C&I:

- Diverse Actuation System design shortfalls were identified within Regulatory Observation RO-UKHPR1000-0001). The RP's application of ALARP principles during the development of solutions to address the identified shortfalls will be followed up by ONR during GDA Steps 3 and 4.

4.6.4 Conclusions

123. Based on the outcome of my Step 2 assessment of ALARP within the C&I safety case, and taking into account the commitments made by the RP to develop and apply a UK HPR1000 ALARP methodology, I have raised no significant shortfalls in this area.

4.7 Out of Scope Items

124. I did not exclude any parts of the C&I design, as defined within Chapter 8 of the PSR and supporting references, from the scope of my sample-based Step 2 assessment. I

considered any aspects of C&I design addressed within chapters of the PSR other than chapter 8 to be out of scope for Step 2.

4.8 Comparison with Standards, Guidance and Relevant Good Practice

125. In Section 2.2 I listed the standards and criteria used to inform my judgement of the adequacy of the standards, guidance and RGP within the GDA Step2 safety case. In this regard, my overall conclusions can be summarised as follows:

- SAPs: I consider that an adequate level of alignment with relevant C&I SAPs is evident from the submissions provided by the RP to enable me to support entry into Step 3 assessment: Table 1 provides further details.
- TAGs: I consider that an adequate level of alignment with C&I TAGs is evident from the submissions provided by the RP to enable me to support entry into Step 3 assessment (e.g. in the overall approach proposed for C&I system classification)
- The high-level international standards and guidance referred to in RP submissions as being applicable to C&I systems important to safety are generally in line with my expectations and UK RGP.

4.9 Interactions with Other Regulators

126. I have had no interactions with other regulators during GDA Step 2.

5 CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

127. During Step 2 of GDA the RP submitted a PSR and other supporting references, which outline a preliminary nuclear safety case for the UK HPR1000. I have performed a sample-based review of these documents. The PSR together with its supporting references present claims in the area of C&I that underpinned the safety of the UK HPR1000.

128. During Step 2 of GDA I have targeted my assessment at the content of the PSR and its references that were of most relevance to the area of C&I, and have assessed against the expectations of ONR's SAPs and TAGs and other guidance which ONR regards as RGP. From the UK HPR1000 assessment performed so far, I have concluded the following:

- Having completed my review of the PSR and supporting documents, I consider my familiarity of the C&I design to have been adequate to support a meaningful Step 2 assessment.

- The information provided on C&I in the PSR related to the design of FCG3, and the PSR stated that the purpose was to '*provide confidence that the I&C systems to be developed for UK HPR1000 will be able to demonstrate compliance with UK regulatory requirements*'. I have concluded that the information provided within the PSR and supporting references did effectively enable me to gain sufficient confidence to complete a meaningful Step 2 assessment.

- One significant issue that I identified during Step 2 concerned shortfalls in the design of the Diverse Actuation System, and I raised a Regulatory Observation to document my concerns. In response, the RP has provided a credible resolution plan setting out a programme of work to address these shortfalls. This was the only Regulatory Observation I raised during Step 2.

- Within GDA Steps 3 and 4, as more safety case documentation is made available by the RP, I will perform further assessment to consider the adequacy of the arguments and evidence which underpin the claims made in Step 2. The substantiation of claims for C&I systems important to safety and consideration of C&I Common Cause Failure are areas of particular interest. I have also identified a number of areas for follow-up within section 4 of this report.

- The RP's strategy for providing a clear structure for C&I Claims Arguments and Evidence was not fully developed in the Step 2 PSR. However, sufficient information was made available to enable a meaningful Step 2 assessment to be performed. The RP has indicated that this aspect of the safety case will be further developed later in the GDA process.

129. Overall, during my GDA assessment of the Step 2 safety case, I have not identified any fundamental safety shortfalls in the area of C&I that might prevent the issue of a Design Acceptance Confirmation (DAC) for the UK HPR1000 design.

5.2 Recommendations

130. My recommendations are as follows.

- Recommendation 1: ONR should consider the outcome of my assessment in deciding whether to proceed to Step 3 of GDA for the UK HPR1000.

- Recommendation 2: All the items identified in this Step 2 report that are described as being ‘items that require follow-up’ should be addressed within the scope of ONR’s GDA Step 3 C&I Assessment Plan for the UK HPR1000.

6 REFERENCES

1. Generic Design Assessment of GNS's UK HPR1000 - Step 2 Assessment Plan for C&I ONR-GDA-AP-17-001, Revision 0, ONR October 2017. TRIM Ref. 2017/351528

2. Preliminary Safety Report (PSR) - Chapter 8 'Instrumentation and Control' - HPR/GDA/PSR/0008 - UK HPR1000, GNS. TRIM Ref. 2017/401358

3. Preliminary Safety Report (PSR) – Chapter 4 General Safety and Design Principles - HPR/GDA/PSR/0004 - UK HPR1000, GNS. TRIM Ref. 2017/401351

4. Supplement to PSR Chapter 8 for HPR1000 (FCG3) Instrumentation & Control Overall Architecture Description - GH X 06000 001 DIYK 03 GN, Rev C, GNS. TRIM Ref. 2018/16944

5. Comparison of HPR1000 (FCG3) Instrumentation and Control Overall Architecture Design With IEC61513 - GH X 06000 001 DIYK 03 TR, Rev E, GNS. TRIM Ref. 2018/35728

6. Safety Claims for Numerical Targets Made on the I&C Systems for HPR1000 (FCG3) - GH X 06000 001 DIKX 03, Rev B, GNS. TRIM Ref. 2018/ 140237.

7. Methodology of Safety Categorisation and Classification - GH X 00100 062 DOZJ 03 GN, GNS. TRIM Ref. 2018/199731

8. ALARP Methodology - GH X 00100 051 DOZJ 03 GN, Ref 0, GNS. TRIM Ref. 2018/181415

9. UK HPR1000 Document Submittal list - Updated versions submitted to the Joint Programme Office (JPO) throughout GDA Step 2, ONR, June 2018. TRIM Ref. 2018/182637

10. Purpose and Scope of Permissioning - NS-PER-GD-014, Revision 6, ONR, Nov 2016. http://www.onr.org.uk/operational/assessment/index.htm

11. Safety Assessment Principles for Nuclear Facilities – SAPs, Revision 0, ONR, 2014. http://www.onr.org.uk/saps/saps2014.pdf

12. Technical Assessment Guides (TAGs)

    Safety Systems - NS-TAST-GD-003, Revision 8, ONR, March 2018

    Demonstration of ALARP - NS-TAST-GD-005, Revision 9, ONR, March 2018

    Safety Related Instrumentation - NS-TAST-GD-031, Revision 4, ONR, July 2014

    Computer Based Safety Systems - NS-TAST-GD-046, Revision 4,ONR, Feb 2017

    Categorisation of Safety Functions and Classification of Structures, Systems and Components - NS-TAST-GD-094, Revision 0, ONR, November 2015

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

13. IAEA guidance

    Safety Classification of Structures, Systems and Components in Nuclear Power Plants, Specific Safety Guide SSG-30, International Atomic Energy Agency (IAEA), 2014

Design of Instrumentation and Control Systems for Nuclear Power Plants, Specific Safety Guide SSG-39, International Atomic Energy Agency (IAEA), 2016

www.iaea.org.

14. Western European Nuclear Regulators' Association (WENRA)

Safety Reactor Safety Reference Levels, WENRA, January 2007

http://www.wenra.org/

15. International Electrotechnical Commission International Standards

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

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

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

http://www.iec.ch/

16. Adequacy of Control and Instrumentation Architecture - Report S.P1893.41.1, Issue 1.0, Altran. TRIM Ref. 2018/256501

17. ONR-Altran Technical Note - Reconciliation of HPR1000 Step 2 Technical Observations, V1.0, Altran, 20th August 2018. TRIM Ref. 2018/272035

18. Pre-Construction Safety Report (PCSR) – Chapter 8 Instrumentation and Control - GH X 00620 008 KPGB 02 GN, Draft Rev B, GNS. TRIM Ref. 2018/105335

19. Generic Design Assessment Guidance to Requesting Parties - ONR-GDA-GD-001 Rev 3, ONR, Sept 2016 www.onr.org.uk/new-reactors/ngn03.pdf

20. GNS UK HPR1000 - UK HPR1000 - Regulatory Query (RQ) Tracking Sheet, ONR. TRIM Ref. 2017/407871

21. GNS UK HPR1000 - UK HPR1000 - Regulatory Observation (RO) Tracking Sheet, ONR. TRIM Ref. 2017/465031

22. RO-UKHPR1000-0001 Diverse Actuation System Design Shortfalls Resolution Plan Rev 0, GNS. TRIM Ref. 2018/170398

23. Summary of the Step 2 Assessment of the UK HPR1000 Reactor, ONR. TRIM Ref. 2018/238474

Table 1

Relevant Safety Assessment Principles Considered During the Assessment

SAP No and Title	Description	Interpretation	Comment
EKP.3, 4 & 5	Engineering Principle: Key principles	EKP.3 – Defence in depth A nuclear facility should be so designed and operated that defence in depth against potentially significant faults or failures is achieved by the provision of several levels of protection. EKP.4 – Safety function The safety function(s) to be delivered within the facility should be identified by a structured analysis. EKP.5 – Safety measures Safety measures should be identified to deliver the required safety function(s).	The implementation of five levels of defence within the C&I architecture is described in Chapter 8 of the PSR (Ref. 2). I have considered this aspect of the design in section 4.2 of this report and raised no shortfalls against this SAP. The identification of safety functions as covered by EKP.4 is considered within the ONR FS assessment (see Summary Report (Ref. 23)) for overview. The C&I architecture design (see section 4.2 for my assessment) contained C&I systems important to safety and it is these systems which I considered to be the EKP.5 'safety measures' with this design.
ECS.1 - 3	Engineering Principle: Safety classification and standards	ECS.1 – Safety Categorisation The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be categorised based on their significance with regard to safety.	See section 4.5 for my consideration of ECS.1 and ECS.2 within the C&I Step 2 safety case. The RP has provided information concerning the categorisation of safety functions based upon nuclear safety significance, however this aspect of the safety case has been assessed within within the FS discipline (see Summary

		ECS.2 – Safety classification of structures, systems and components Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance with regard to safety. ECS.3 - 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 standards.	Report (Ref. 23) for overview). My consideration of the RP's approach to the classification of C&I systems (ECS.2) is covered section 4.5. I was content that the high-level information provided in the safety case generally aligned with the requirements of the SAPs The Step 2 safety case identifies a number of international standards as being used to develop FCG3 C&I. See section 4.8 for my consideration of this aspect (ECS.3) of the Step 2 safety case. The high-level standards referenced in the safety case aligned with my expectations.
EQU.1	Engineering Principle: Equipment qualification	EQU.1 – Qualification Procedures Qualification procedures should be in place to confirm that structures, systems and components that are important to safety will perform their required safety function(s) throughout their operational lives.	Chapter 8 of the PSR (Ref. 2) described in principle how systems would be qualified for their environmental duties, and this approach aligned with my expectations, but no detailed assessment of this aspect of the design has been performed in Step 2 – to be considered later in the GDA process.
EDR.1, 2, 3, 4	Engineering Principle: Design for reliability	EDR.1 Due account should be taken of the need for structures, systems and components important to safety to be designed to be inherently safe or to fail in a safe manner and potential failure modes should be identified, using a formal	These principles informed my assessment of the C&I architecture and C&I systems as reported in sections 4.2 and 4.3 respectively. In particular, EDR.1 and EDR.3 informed my development of RO-UKHPR1000-0001 Diverse Actuation System Design Shortfalls (Ref. 20), section 4.3.

		analysis where appropriate. EDR. 2 Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components important to safety. EDR. 3 Common cause failure (CCF) should be explicitly addressed where a structure, system or component important to safety employs redundant or diverse components, measurements or actions to provide high reliability. EDR. 4 During any normally permissible state of plant availability, no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function.	
ERL.3	Engineering Principle: Reliability claims	ERL.3 The reliability claimed for any structure, system or component important to safety should take into account its novelty, the experience relevant to its proposed environment, and the uncertainties in operating and fault conditions, physical data and design methods.	This SAP informed my assessment of C&I system reliability claims as described in Section 4.4. This aspect of the safety case will be considered in greater detail later in the GDA process.

ECM.1	Engineering Principle: Commissioning	ECM.1 Before operating any facility or process that may affect safety it should be subject to commissioning tests to demonstrate that, as built, the design intent claimed in the safety case has been achieved.	Chapter 8 of the PSR describes how HMI facilities will be provided to enable C&I commissioning. The adequacy of commissioning testing was not considered within GDA Step 2.
EMT. 7	Engineering Principle: Maintenance, inspection and testing	EMT.7 In-service functional testing of systems, structures and components important to safety should prove the complete system and the safety-related function of each component	This SAP informed my assessment of C&I systems as covered by section 4.3. Chapter 8 of the PSR (Ref. 2) stated that Class 1 and Class 2 systems I&C systems are designed to permit periodic testing in order to confirm their ability to perform their required functions. This high-level claim aligned with my expectations.
EAD.1	Engineering Principle: Ageing and degradation	EAD.1 The safe working life of structures, systems and components that are important to safety should be evaluated and defined at the design stage.	This SAP informed my assessment of C&I systems as covered by section 4.3. Chapter 8 of the PSR (Ref. 2) stated the high level claim that 'the effects of ageing of each system have been addressed in the design'. I did not perform any detailed assessment of this claim during Step 2.
ELO.1	Engineering Principle: Layout	ELO.1 The design and layout should facilitate access for necessary activities and minimise adverse interactions during such activities.	This SAP informed my assessment of C&I architecture as covered by section 4.2. Chapter 8 of the PSR (Ref. 2) described in general terms how factors such as physical separation, transportation, installation, maintenance, convenience and expandability have been taken into account in I&C equipment layout. I considered that this high-level statement of the design approach was sufficient to support my Step 2 assessment.
EHA.1	Engineering Principle:	EHA.1	The adequacy of the Step 2 safety case

	External and internal hazards	External and internal hazards that could affect the safety of the facility should be identified and treated as events that can give rise to possible initiating faults.	regarding faults initiated by external and internal hazards has been assessed by ONR hazard disciplines (please refer to the Step 2 Summary Report (Ref. 23) for overview). The qualification of C&I equipment to withstand UK HPR1000 environmental operating conditions is considered under EQU.1 above.
ESS.1, 2, 3, 7, 8, 18, 21, 23, 27	Engineering Principle: Safety systems	ESS.1 - Requirement for safety systems All nuclear facilities should be provided with safety systems that reduce the frequency or limit the consequences of fault sequences, and that achieve and maintain a defined safe state. ESS.2 - Determination of safety system requirements The extent of safety system provisions, their functions, levels of protection necessary to achieve defence in depth and required reliabilities should be determined ESS.3 - Monitoring of plant safety Adequate provisions should be made to enable the monitoring of the plant state in relation to safety and to enable the taking of any necessary safety actions. ESS.7 - Diversity in the detection of fault sequences	These SAPs informed my assessment of safety systems (i.e. Class 1 systems) as reported under sections 4.2 and 4.3 of this report.

		The protection system should employ diversity in the detection of fault sequences, preferably by the use of different variables, and in the initiation of the safety system action to terminate the sequences. ESS.8 - Automatic initiation A safety system should be automatically initiated and normally no human intervention should be necessary following the start of a requirement for protective action. ESS.18 - Failure independence No fault, internal or external hazard should disable a safety system. ESS.21 – Reliability The design of a safety system should avoid complexity, apply a fail-safe approach and incorporate the means of revealing internal faults from the time of their occurrence. ESS.23 - Allowance for unavailability of equipment. In determining the safety system provisions, allowance should be made for the unavailability of equipment. ESS.27 - Computer-based safety systems Where the system reliability is significantly dependent upon the performance of computer software, the establishment of and compliance	

		with appropriate standards and practices throughout the software development life-cycle should be made, commensurate with the level of reliability required, by a demonstration of 'production excellence' and 'confidence-building' measures.	
ESR.1, 3, 5	Engineering Principle: Control and instrumentation of safety-related systems	ESR.1 - Provision in control rooms and other locations Suitable and sufficient safety-related system control and instrumentation should be available to the facility operator in a central control room, and as necessary at appropriate locations on the facility. ESR.3 - Provision of controls Adequate and reliable controls should be provided to maintain variables within specified ranges ESR.5 - Standards for computer based equipment Where computers or programmable devices are used in safety-related systems, evidence should be provided that the hardware and software are designed, manufactured and installed to appropriate standards.	These SAPs informed by assessment of C&I safety related systems (i.e. Class 2 and 3) as reported under sections 4.2 and 4.3 of this report. Note: Assessment of the adequacy of control room facilities (ESR.1) has been led by the ONR HF discipline, as summarised in the Step 2 Summary Report (Ref.23).
EES	Engineering Principle: Essential services	EES.1 - Provision Essential services should be provided to	Chapter 8 of the PSR (Ref. 2) describes the provision of support services in general terms (e.g. electrical supplies, Heating and

		ensure the maintenance of a safe plant state in normal operation and fault conditions.	Ventilation). The ONR's assessment of the adequacy of the Step 2 safety case for such services is summarised in the Step 2 Summary Report (Ref. 23).
ECV	Engineering principles: containment and ventilation: containment monitoring	ECV.6 – Monitoring devices Suitable monitoring devices with alarms and provisions for sampling should be provided to detect and assess changes in the stored radioactive substances or changes in the radioactivity of the materials within the containment. ECV.7 – Leakage monitoring Appropriate sampling and monitoring systems and other provisions should be provided outside the containment to detect, locate, quantify and monitor leakages of nuclear matter from the containment boundaries under normal and accident conditions.	Chapter 8 of PSR (Ref. 2) describes the provision of radiation monitoring systems in general terms, e.g. provision of a Plant Radiation Monitoring System. This information was sufficient to support my C&I assessment. The adequacy of the proposed UK HPR1000 radiation monitoring facilities and leakage monitoring has been considered in more detail within the ONR Radiological Protection Step 2 assessment, as summarised in the Step 2 summary report (Ref. 23).