Office for Nuclear Regulation

New Reactors Division – Generic Design Assessment

Step 4 Assessment of Cross-cutting Topics for the UK HPR1000 Reactor

Assessment Report ONR-NR-AR-21-007
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 six cross-cutting aspects of the UK HPR1000 reactor design undertaken as part of the Office for Nuclear Regulation's (ONR) Generic Design Assessment (GDA). Cross-cutting topics are those that have a bearing on a wide range of the disciplines assessed by ONR in GDA, and therefore benefit from adopting a holistic approach to their assessment. The six cross-cutting topics covered in this report are:

- Nuclear Safety Principles (NSPs) underpinning the generic UK HPR1000 design and safety case.
- Development of the generic UK HPR1000 safety case.
- Management of commitments in the UK HPR1000 GDA.
- Management of implementable requirements and assumptions in the generic UK HPR1000 safety case.
- Approach to operating rules for UK HPR1000.
- Use of Operating Experience (OPEX) in the generic UK HPR1000 design and safety case.

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 on the adequacy of the six cross-cutting topics listed above and on whether, from the perspective of those topics, 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 information contained within the PCSR and supporting documentation regarding the six cross-cutting topics.

My assessment focussed on the following aspects of the generic UK HPR1000 safety case:

- The general safety and design principles described in Chapter 4 of the PCSR which are the NSPs underpinning the UK HPR1000.
- The RP's approach to producing, developing and delivering the generic UK HPR1000 safety case throughout GDA, including the RP's organisational capability.
- The RP's commitments management process for identifying, capturing and managing commitments throughout GDA. This included the appropriate capture of post-GDA commitments to be considered by the licensee.
- The RP's arrangements for identifying and tracing requirements and assumptions throughout the safety case. This included a detailed sampling of the implementation of the RP's requirements management process.
- The RP's approach to developing and identifying operating rules within the generic UK HPR1000 safety case and its suitability for transfer to a licensee.
- The RP's demonstration of how OPEX is identified, captured, and used in the UK HPR1000 design.

The conclusions from my assessment of the six cross-cutting topics are:

- The safety case for the above cross-cutting topics, which comprises Chapters 4, 20 and 31 of the PCSR plus the supporting evidence, has been adequately developed for the purposes of GDA.
- The UK HPR1000 general safety and design principles are adequate for the purposes of GDA.
- The RP established and deployed suitable means to deliver, in a timely manner, a comprehensive safety case.
- The RP established adequate arrangements for capturing and implementing commitments during GDA. The RP has identified and captured post-GDA commitments for the licensee to consider.
- The RP's process for identifying and tracing requirements through the generic UK HPR1000 safety case is adequate for the purposes of GDA. This process is at an early stage and it needs further development by a licensee.
- The RP's approach for defining operating rules underpinned by the safety case is sufficient for GDA and suitable for further development by a licensee.
- The RP has developed adequate arrangements for identifying, capturing and analysing OPEX, including a suitable and sufficient new OPEX methodology.

These conclusions are based upon the following factors:

- A detailed and in-depth assessment, on a sampling basis, of the full scope of safety submissions at all levels of the hierarchy of the generic UK HPR1000 safety case documentation.
- Detailed technical interactions with the RP, including technical workshops alongside other disciplines.
- Assessment of the responses to the Regulatory Queries and Regulatory Observations 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 six 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 the perspective of the cross-cutting topics covered in this report a DAC may be granted.

LIST OF ABBREVIATIONS

ALARP	As Low As Reasonably Practicable
ASG [EFWS]	Emergency Feedwater System
BAT	Best Available Techniques
BFX	Fuel Building
BMS	Business Management System
BoSC	Basis of Safety Case
BRB	Bradwell Power Generation Company Limited
BRX	Reactor Building
C&I	Control and Instrumentation
CGN	China General Nuclear Power Corporation Ltd
CRS	Chemical and Radiochemical Specification
DAC	Design Acceptance Confirmation
DBC	Design Basis Condition
DCL [MCRACS]	Main Control Room Air Conditioning System
DEC	Design Extension Condition
DFR	Duty Functional Requirement
DiD	Defence in Depth
DL	Document List
DSR	Design Substantiation Report
EMIT	Examination. Maintenance, Inspection and Testing
ETS	Environmental Technical Specification
FAP	(RP's) Forward Action Plan
FFR	Fault Functional Requirement
GDA	Generic Design Assessment
GNI	General Nuclear International Ltd.
GNSL	General Nuclear System Ltd.
GSR	Generic Security Report
HBSC	Human Based Safety Claims
HEPF	High Energy Pipe Failure
HOW2	(ONR) Business Management System
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
ID	Identifier
IDP	Integrated Delivery Plan
IDT	Integrated Delivery Tool
IPR	Intellectual Property Rights

IRWST	In-containment Refuelling Water Storage Tank
ISI	In-service Inspection
ISO	International Organisation for Standardisation
MDSL	Master Document Submission List
MSQA	Management for Safety and Quality Assurance
MW	Megawatts
NPP	Nuclear Power Plant
NSP(s)	Nuclear Safety Principle(s)
OFR	Other Functional Requirements
ONR	Office for Nuclear Regulation
OPEX	Operational Experience
OTS	Operational Technical Specification
PCER	Pre-construction Environmental Report
PCSR	Pre-construction Safety Report
PIE	Postulated Initiating Event
PM	Preventative Maintenance
PSA	Probabilistic Safety Analysis
PSR	Periodic Safety Review
PT	Periodic Testing
PTCN	Periodic Test Completeness Note
PTR [FPCTS]	Fuel Pool Cooling and Treatment System
PWR	Pressurised Water Reactor
RC	Reinforced Concrete
RCC-M	Règles de Conception et de Construction des Matériels Mècaniques des Ilots Nucléaires PWR
RGP	Relevant Good Practice
RHR	Residual Heat Removal
RIS [SIS]	Safety Injection System
RO	Regulatory Observation
RP	Requesting Party
RPS [PS]	Protection System
RQ	Regulatory Query
SAP(s)	Safety Assessment Principle(s)
SAR	Safety Assessment Report
SCDM	Safety Case Development Manual
SDM	System Design Manual
SFAIRP	So Far As Is Reasonably Practicable
SFIS	Spent Fuel Interim Storage

SFP	Spent Fuel Pool
SFRR	Safety Functional Requirements Report
SoDA	(Environment Agency's) Statement of Design Acceptability
SQEP	Suitably Qualified and Experienced Personnel
SSC(s)	Structures, Systems and Components
SSER	Safety, Security and Environmental Report
TAG	Technical Assessment Guide
TS	Technical Specification
TSC	Technical Support Contractor
US NRC	United States Nuclear Regulatory Commission
WENRA	Western European Nuclear Regulators' Association

TABLE OF CONTENTS

Tables

Figures

Annexes

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, of a number of topics of a cross-cutting nature, implying that they are related to, and have a significance to, a wide range of the disciplines assessed by ONR in GDA and, therefore, benefit from adopting a holistic approach to their assessment. The cross-cutting topics covered by my assessment are:

   - Nuclear Safety Principles (NSPs) underpinning the generic UK HPR1000 design and safety case.
   - Development of the generic UK HPR1000 safety case.
   - Management of commitments in the UK HPR1000 GDA.
   - Management of implementable requirements and assumptions in the generic UK HPR1000 safety case.
   - Approach to operating rules for UK HPR1000.
   - Use of Operating Experience (OPEX) in the generic UK HPR1000 design and safety case.

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, which commenced in 2017, followed a step-wise approach in a claims-argument-evidence hierarchy. Major technical interactions started in Step 2 of the GDA which focussed on an examination of the main claims made by the RP for the UK HPR1000. In Step 3 of the GDA, the arguments which underpin those claims were examined. The GDA Step 2 reports for individual technical areas, and the summary reports for GDA Steps 2 and 3 are published on the joint regulators' website. The objective of Step 4 of the GDA 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 traceable through the safety case.
   - 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 identifying paths for resolution.

6. During GDA a number of cross-cutting topics, which were significant enough to warrant dedicated management focus, leadership and coordination, were identified by ONR (see full list in Annex 3). The assessments undertaken for the majority of those cross-cutting topics, and conclusions reached, are reported, as appropriate, in the relevant discipline assessment reports (Ref. 3) and summarised in the GDA Step 4 summary report (Ref. 4). However, several of the cross-cutting topics relate to arrangements and methodologies and those apply to all the disciplines, thus, centralised reporting was deemed more appropriate. Therefore, those cross-cutting topics are reported in this assessment report and summarised in the GDA Step 4 summary report (Ref. 4) .

7. The cross-cutting topics reported in this assessment report are:

- NSPs underpinning the generic UK HPR1000 design and safety case. For simplicity this cross-cutting topic will be referred to as 'NSPs'.
- Development of the generic UK HPR1000 safety case. For simplicity this cross-cutting topic will be referred to as 'safety case development'.
- Management of commitments in the UK HPR1000 GDA. For simplicity this cross-cutting topic will be referred to as 'commitments management'.
- Management of implementable requirements and assumptions in the generic UK HPR1000 safety case. For simplicity this cross-cutting topic will be referred to as 'safety case requirements management'.
- Approach to operating rules for UK HPR1000. For simplicity this cross-cutting topic will be referred to as 'approach to operating rules'.
- Use of OPEX in the generic UK HPR1000 design and safety case. For simplicity this cross-cutting topic will be referred to as 'OPEX arrangements'.

8. The purpose of this report is therefore to summarise my assessment in the above cross-cutting topics which provides an input to ONR's 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

9. This report presents the findings of my assessment of six cross-cutting aspects of the generic UK HPR1000 design listed in the above section, which has been undertaken as part of GDA. I carried out my assessment using the Pre-construction Safety Report (PCSR) (Ref. 5, Ref. 6, Ref. 7) and supporting documentation submitted by the RP. My assessment was focussed on considering whether the generic safety case provides an adequate justification for the generic UK HPR1000 design, in line with the objectives for GDA.

1.3 Methodology

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

11. My assessment was undertaken in accordance with the requirements of ONR's How2 Business Management System (BMS). ONR's SAPs (Ref. 2), together with supporting Technical Assessment Guides (TAGs), were used as the basis for my assessment. Further details are provided in Section 2. The outputs from my assessment are consistent with ONR's GDA guidance to RPs (Ref. 1).

2 ASSESSMENT STRATEGY

12. The strategy for my assessment is set out in this section. This section identifies the general strategy adopted, the scope covered in this report and the standards and criteria that have been applied for the assessment.

13. Throughout GDA, 22 multi-disciplinary and cross-cutting topics were identified which were significant enough to warrant dedicated management focus, leadership and coordination.

14. Annex 3 provides the full list of the cross-cutting topics. In addition, cross-cutting topics are summarised in the GDA Step 4 summary report (Ref. 4).

2.1 Assessment Scope

15. This sub-section provides a high-level overview of each of the six cross-cutting topics covered in this report:

- NSPs – The scope of my assessment was limited to the adequacy of the RP's nuclear safety principles, in terms of alignment with relevant good practice (RGP) and completeness.
- Safety case development – The scope of my assessment was largely associated with the RP adequately addressing RO-UKHPR1000-0004, 'Development of a Suitable and Sufficient Safety Case' Actions 1 to 3 (Ref. 9). This included the assessment of the RP's approach for producing, developing and delivering the generic UK HPR1000 safety case throughout GDA. I also assessed the RP's organisational capability to produce and develop the generic UK HPR1000 safety case and the programme to deliver the safety case.
- Commitments management – The scope of my assessment included the RP's approach to ensuring that safety related commitments were identified, appropriately captured and managed for implementation during GDA or, where appropriate, to be supplied to the licensee. This included assessing the RP's commitments procedure and sampling the approach adopted.
- Safety case requirements management – The scope of my assessment included the RP's approach to ensuring that safety related assumptions and requirements are identified within the safety case, appropriately captured and managed throughout GDA, and capable of being supplied to the licensee. This included assessing the RP's requirements management procedures and assessing the RP's evidence to demonstrate application of the requirements management arrangements. This last point was done through the assessment of ten examples in the GDA design.
- Approach to operating rules – The scope of my assessment included the RP's approach to identifying and managing operating rules and how those were underpinned by its safety case. I also focused on the suitability of the operating rules arrangements for transfer to a licensee in a manner that facilitates its understanding and further development.
- OPEX arrangements – The scope of my assessment was largely associated with the RP adequately addressing RO-UKHPR1000-0044, 'Identification and Use of Operational Experience (OPEX) in the UK HPR1000 Generic Design and Safety Case' (Ref. 10). My assessment included the RP's arrangements for identifying, capturing and justifying the applicability of relevant OPEX and the RP's demonstration of suitable and sufficient integration of relevant OPEX into the generic UK HPR1000 safety case.

16. I considered all the main submissions associated with the above cross-cutting topics within the remit of my assessment scope, to various degrees of breadth and depth. I chose to concentrate my assessment on those aspects that I judged to have the

greatest safety significance. My assessment was also influenced by the claims made by the RP, my previous experience of similar arrangements 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 RQs and ROs I raised as a result of my on-going assessment, and the resolution thereof.

2.2 Sampling Strategy

17. In line with ONR's guidance (Ref. 8), I chose a sample of the RP's submissions to undertake my assessment. The main themes considered for each of the cross-cutting topics covered in this report were:

- Nuclear safety principles:
  - My sample included the NSPs within PCSR Chapter 4 (Ref. 5) and the General Safety Requirements (Ref. 11).
  - Comparison between ONR's SAPs and the RP's NSPs.
  - Assessment of the RQs' responses relevant to this cross-cutting topic (Ref. 12).
- Safety case development:
  - Assessment of the relevant sections of PCSR Chapter 20 (Ref. 6).
  - Assessment of the RP's safety case strategy (Ref. 13) and RP's tools to demonstrate that the strategy could be enacted. Further details of the RP's submissions and my sample are provided in sub-section 4.3.
  - Assessment of the RP's demonstration of the adequacy of the organisation that is in place to produce and develop the generic UK HPR1000 safety case throughout GDA.
  - Assessment of the RQs' responses relevant to this cross-cutting topic (Ref. 12).
- Commitments management:
  - Assessment of the relevant section of PCSR Chapter 20 (Ref. 6).
  - Assessment of the RP's commitments management approach and procedure (Ref. 14) for identifying, capturing, and managing commitments. Details of the RP's submissions and my sample are provided in sub-section 4.4.
  - Post-GDA commitments' identification and arrangements for supplying them to the licensee (Ref. 15).
  - Assessment of the RQs' responses relevant to this cross-cutting topic . (Ref. 12).
- Safety case requirements management:
  - Assessment of the relevant section of PCSR Chapter 20 (Ref. 6).
  - Assessment of the RP's approach and arrangements for the identification and traceability of requirements and assumptions through the safety case (Ref. 16, Ref. 17). Details of the RP's submissions and my sample are provided in sub-section 4.5.
  - Assessment of the RP's requirements management examples. Details of those examples are provided in sub-section 4.5.
  - Assessment of the RQs' responses relevant to this cross-cutting topic (Ref. 12).

- Approach to operating rules:
  - Assessment of RP's approach to operating rules which is summarised in PCSR Chapter 31 (Ref. 7) and described in more detailed in the 'Generic Limits and Conditions for Normal Operation' (Ref. 18). Details of further RP's submissions are provided in sub-section 4.6.
  - Sampling the derivation of operating rules for a system, the Safety Injection System (RIS [SIS]) (Ref. 19). See sub-section 4.6 for further details.
  - Assessment of the RQ's response on this cross-cutting topic (Ref. 12).
- OPEX arrangements:
  - Assessment of the relevant section of the PCSR Chapter 20 (Ref. 6).
  - Assessment of the RP's existing procedure (Ref. 20) and new methodology (Ref. 21) for the use of OPEX. Details of the RP's submissions are provided in sub-section 4.7.
  - Assessment of the RP's demonstration of the OPEX arrangements including the identification of OPEX dependent topics, identification of gaps in the RP's existing arrangements, and the practical application of the new OPEX methodology.
  - Assessment of the RQ's response on this cross-cutting topic. (Ref. 12).

2.3 Out of Scope Items

18. The following items were outside the scope of my assessment:

- NSPs:
  - I have not considered the application of the NSPs to the design as this was taken into account, where appropriate, by the individual technical disciplines in ONR.
  - Similarly, the security and environmental principles which are reported in the Generic Security Report (GSR) and the Pre-construction Environmental Report (PCER) were outside of the scope of my assessment.
- Safety case development:
  - I have not considered the technical adequacy of the safety case as this was assessed at a discipline level and reported in the GDA Step 4 discipline assessment reports.
- Commitments management:
  - I have not considered the technical adequacy of any commitments identified by the RP. This was considered at the discipline level, as appropriate.
- Safety case requirements management:
  - I have not considered whether the specific requirements identified are adequate or complete as this requires a detailed knowledge across a range of different technical disciplines. This aspect was addressed by the individual discipline assessments, as appropriate.

- I have not considered the overall adequacy of the engineering or operational documentation that contains the requirements, over and above them being used as a mechanism to identify and trace requirements through the safety case. Again, this was considered within individual technical disciplines, as appropriate.

- Approach to operating rules:

  - I have not considered whether the specific operating rules identified are adequate or complete and I have not considered the scope of operating rules defined for a given discipline. These require a detailed knowledge of the safety case across a range of different technical disciplines and were addressed by the individual discipline assessments, as appropriate.
  - There is an interface with environmental requirements and specifications, and the RP commonly refers to 'safety' operating rules to also encompass environmental aspects. I have not assessed any aspects which are solely related to environmental operating rules, and where there is such an overlap my assessment is only applicable to safety considerations.
  - Any operational documentation that allows the identified operating rules to be implemented have not been considered. This is a licensee choice over how to best implement the operating rules within its chosen documentation structure. However, where I have identified shortfalls in what is proposed by the RP, these are noted.
  - There is an overlap with RO-UKHPR1000-0021 (Ref. 22) which deals with the Examination, Maintenance, Inspection and Testing (EMIT) arrangements for the UK HPR1000 during GDA. I did not assess any aspects under the scope of this RO.

- OPEX arrangements:

  - I have not considered detailed assessment of the RP's approach to identifying and using OPEX across all topics.
  - I have not considered whether OPEX is suitable and sufficient to support the claims and arguments in the generic UK HPR1000 safety case. These judgements are matters for ONR's specialists in individual technical topics to consider.
  - I have not assessed the adequacy of the RP's arrangements for training personnel on OPEX-related matters.

2.4 Standards and Criteria

19. The relevant standards and criteria adopted within this assessment are principally the SAPs (Ref. 2), TAGs, relevant national and international standards, and RGP 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 Assessment Principles

20. The SAPs (Ref. 2) constitute the regulatory principles against which ONR judge the adequacy of the safety case. The SAPs applicable to each of the six cross-cutting topics are included within Annex 1 of this report.

21. My assessment of the RP's NSPs used the majority of the SAPs, with the exception of the siting SAPs.

22. The key SAPs applied within my assessment of the safety case development, commitments management and safety case requirements management were SAPs SC.1, SC.2, SC.4, SC.6, SC.7, SC.8, ECS.3, ECE.12, ECV.2, ECV.3 and EMT.1.

23. The key SAPs applied within my assessment of the RP's approach to operating rules were SAPs SC.4 and SC.6.

24. The key SAPs applied within my assessment of the OPEX arrangements were SAPs MS.4 and SC.7.

2.4.2 Technical Assessment Guides

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

- NS-TAST-GD-005, 'ONR Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable)' (Ref. 23)
- NS-TAST-GD-009, 'Examination, Inspection, Maintenance and Testing of Items Important to Safety' (Ref. 24)
- NS-TAST-GD-035, 'Limits and Conditions for Nuclear Safety (Operating Rules)' (Ref. 25)
- NS-TAST-GD-050, 'Periodic Safety Reviews (PSR)' (Ref. 26)
- NS-TAST-GD-051, 'The Purpose, Scope and Content of Nuclear Safety Cases' (Ref. 27)
- NS-TAST-GD-096, 'Guidance on Mechanics of Assessment' (Ref. 8)

2.4.3 National and International Standards and Guidance

26. The following standards and guidance were used as part of this assessment:

- International Atomic Energy Agency (IAEA) – Safety Standards: 'Fundamental Safety Principles', No. SF-1 (Ref. 28)
- IAEA – Safety Standards: 'Safety of Nuclear Power Plants: Design', Specific Safety Requirements No. SSR-2/1 (Rev.1) (Ref. 29)
- IAEA – Safety Standards: 'Safety of Nuclear Power Plants: Commissioning and Operation', Specific Safety Requirements No. SSR-2/2' (Rev.1) (Ref. 30)
- IAEA – Safety Standards: 'Leadership and Management for Safety', General Safety Requirements No. GSR Part 2' (Ref. 31)
- IAEA – Safety Standards: 'Safety Classification of Structures, Systems and Components in Nuclear Power Plants', Specific Safety Guide No.SSG-30 (Ref. 32)
- IAEA – Safety Standards: 'Deterministic Safety Analysis for Nuclear Power Plants', Specific Safety Guide No. SSG-2 (Rev. 1) (Ref. 33)
- IAEA – Safety Standards: 'Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants', Safety Guide NS-G-2.2 (Ref. 34)
- Western European Nuclear Regulators' Association (WENRA), 'Report - Safety of New Nuclear Power Plant Designs' (Ref. 35)
- WENRA, 'Safety Reference Levels for Existing Reactors 2020' (Ref. 36)

2.5 Integration with Other Assessment Topics

27. GDA requires the submission of an adequate, coherent and holistic generic safety case. Regulatory assessment cannot be carried out in isolation as there are often issues that span multiple disciplines. The majority of the cross-cutting topics discussed in this report impact all the other disciplines, and so they have been involved or

provided input to my assessment. I have therefore worked closely with a number of ONR inspectors and the Environment Agency to inform my assessment. The key interactions were:

- All technical disciplines contributed to the 'safety case health check' that informed my assessment of the safety and security case development.
- During my assessment of the safety case requirements management, I sought input and provided feedback to a number of disciplines to ensure consistency and alignment. Notably this included close interactions with Mechanical Engineering, Control and Instrumentation (C&I) and Fault Studies inspectors.
- Management for Safety and Quality Assurance (MSQA) – I worked closely with the MSQA inspector during the assessment of the RP's arrangements for managing commitments and safety case requirements. Regarding the OPEX assessment, the MSQA inspector and the Environment Agency MSQA lead sought evidence for how the RP's OPEX arrangements were implemented in practice and I used their input in my assessment.
- Assessing how OPEX is identified and used is cross-cutting and wide reaching. However, some topics place a greater emphasis on OPEX in making an adequate demonstration of safety. Therefore, during my assessment of the use of OPEX, I worked closely with Chemistry, Human Factors, MSQA, Radiological Protection and Nuclear Liabilities Regulation inspectors.
- The Environment Agency, in particular the lead assessor for MSQA, who jointly with ONR's MSQA inspector assessed the RP's deliverables for the demonstration of the arrangements for identifying, capturing and justifying the applicability of relevant OPEX.

3 REQUESTING PARTY'S SAFETY CASE

3.1 Introduction to the Generic UK HPR1000 Design

28. The generic UK HPR1000 design is described in detail in the PCSR (Ref. 5) It is a three-loop PWR designed by CGN using the Chinese Hualong technology. The generic UK HPR1000 design has evolved from reactors which have been constructed and operated in China since the late 1980's, 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 generic UK HPR1000 design is claimed to have a lifetime of at least 60 years and has a nominal electric output of 1,180 MW.

29. The reactor core contains zirconium clad uranium dioxide (UO2) 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.

30. The Reactor Building (BRX) 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 BRX and house key safety systems and the main control room. The Fuel Building (BFX) 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.

3.2 The Generic UK HPR1000 Safety Case

31. The RP's documentation underpinning the PCSR is arranged in a tiered structure. The PCSR is the tier 1 document. The key documents describing the design, design bases, methodologies and key processes are tier 2 documents. The further documents required to provide detailed supporting evidence are tier 3 documents. The document hierarchy is described within the RP's safety case development strategy (Ref. 13) and in the production strategies for each technical discipline.

32. The UK HPR1000 has one overarching safety objective according to PCSR Chapter 1 (Ref. 5). This is that the "generic UK HPR1000 could be constructed, operated, and decommissioned in the UK on a site bounded by the generic site envelope in a way that is safe, secure and that protects people and the environment". The RP has defined a series of high-level claims to provide structure to its safety case. The link between this safety objective, the high-level claims and the different cross-cutting topics is explained in each of the sub-sections below.

33. In this section, I also provide an overview of the RP's generic UK HPR1000 safety case as provided during GDA for the six cross-cutting topics covered in this report.

34. Details of the technical content of the documentation and my assessment of its adequacy are reported in the subsequent sections of my report.

3.2.1 Nuclear Safety Principles

35. PCSR Chapter 4 'General Safety and Design Principles' (Ref. 5) describes the nuclear safety principles underpinning the generic UK HPR1000 design and supports the overarching safety objective through the high-level claim 2 and sub-claim 2.3:

- Claim 2: "The UK HPR1000 design will be developed in an evolutionary manner, using a robust design process, building on relevant good international practice, to achieve a strong safety and environmental performance".
- Sub-claim 2.3: "Suitable General Safety and Design Principles are in place to ensure the design meets the nuclear safety objective".

36. The RP identified two arguments to support the above sub-claim (Sub-claim 2.3) which are summarised below:

- The NSPs have been developed considering Chinese nuclear regulatory requirements, international good practice and the UK context.
- The NSPs are developed with a logical process to be applied to the design to achieve the nuclear safety objective.

37. The RP provided evidence, in terms of references to international good practice and UK context to support the first argument. To support the second argument, the RP provided an overview of the NSPs highlighting how they support the nuclear safety objective.

38. The main tier 2 document supporting Chapter 4 of the PCSR is the RP's 'General Safety Requirements' report (Ref. 11).

3.2.2 Safety Case Development

39. PCSR Chapter 20 'MSQA and Safety Case Management' (Ref. 6) covers the RP's arrangements for managing the safety case including safety case consolidation. This chapter supports claim 2 (see above) and sub-claim 2.2: "Suitable organisational arrangements are in place for the development & substantiation of the UK HPR1000"

40. Chapter 20 of the PCSR describes, at a high-level, the arrangements and tools in place to develop and deliver a good quality and comprehensive safety case. This chapter references key tier 2 documents, such as the 'Safety Case Development Strategy' (Ref. 13) and the 'Safety Case Development Manual' (Ref. 37). Chapter 20 also provides an overview of the safety case management organisation that was in place to deliver the safety case. There are also references to the RP's procedures for the production and technical review of work (Ref. 38).

3.2.3 Commitments Management

41. PCSR Chapter 20 'MSQA and Safety Case Management' (Ref. 6) covers the RP's arrangements for managing the safety case commitments.

42. Sub-section 20.5.9 of PCSR Chapter 20 provides an overview to the safety case commitments management process and refers to the 'Management of Commitments for Safety Case Updates' procedure (Ref. 39) and the CGN internal procedure (Ref. 14). This PCSR section mentions a 'commitments log' and states that there is a process for identifying, recording and managing post-GDA commitments. The tier 2 document supporting this is the 'Post-GDA commitment list' (Ref. 15).

3.2.4 Safety Case Requirements Management

43. PCSR Chapter 20 'MSQA and Safety Case Management' (Ref. 6), includes a high-level summary section to introduce the development of the safety case requirements management process implemented for the UK HPR1000 GDA project.

44. There are two RP's documents that describe the requirements management arrangements: a tier 2 document, 'Requirements Management Summary' report (Ref. 16) and the 'Requirements Management Regulations' (Ref. 17), a tier 2 document. The remainder of the RP's safety case is comprised of a significant number of tier 2 and tier 3 documents that are described in more detail in sub-section 4.5.

3.2.5 Approach to Operating Rules

45. PCSR Chapter 31 'Operational Management' (Ref. 7) presents the RP's approach for operational management. This PCSR chapter also details the substantiation of the safety aspects of operation and management to ensure that relevant safety case requirements are identified in the operating rules. This chapter includes operating rules, amongst other aspects, and summarises the methodology and principles adopted during GDA. This chapter supports claim 3 and sub-claims 3.3 and 3.3.15:

- Claim 3: "The design and intended construction and operation of the UK HPR1000 will protect the workers and the public by providing multiple levels of defence to fulfil the fundamental safety functions, reducing the nuclear safety risks to a level that is as low as reasonably practicable".
- Sub-claim 3.3: "The design of the processes and systems has been substantiated and the safety aspects of operation and management have been substantiated".
- Sub-claim 3.3.15: "The safety aspects of operational management have been substantiated".

46. The RP identifies several arguments to support sub-claim 3.3.15, but the most relevant one regarding operating rules is that "the most significant operating limits and conditions are identified to ensure the plant is operated safely at all times". The evidence that the RP cites to support this argument is presented in sub-section 31.5 of Chapter 31 of the PCSR (Ref. 7). The PCSR presents the general approach adopted by the RP with more detailed information on key limits presented in 'Generic Limits and Conditions for Normal Operation' (Ref. 18). There are several documents underpinning the RP's approach (Ref. 18), and I have sampled one of them, the 'Operational Technical Specification (OTS) for the Safety Injection System (RIS)[SIS]' (Ref. 19).

47. Note that throughout its submissions the RP uses the umbrella term of 'operating limits and conditions'. The RP's definitions differ slightly from ONR's terminology as per NS-TAST-GD-035 (Ref. 25). Therefore, to avoid ambiguity I refer to operating rules throughout my assessment, as defined by the ONR TAG.

3.2.6 OPEX Arrangements

48. PCSR Chapter 20 'MSQA and Safety Case Management' (Ref. 6) includes a high-level section on the OPEX arrangements for the UK HPR1000. This section refers to the RP's existing OPEX arrangements (Ref. 20) and to the RP's new OPEX methodology (Ref. 21) which supplements the existing arrangements. Those references are tier 2 documents.

49. The remainder of the safety case is comprised of the topic specific OPEX reports, which are key supporting reports for the RP's demonstration, at a topic level, that the relevant risks have been reduced to ALARP (referred to as 'ALARP demonstration').

4 ONR ASSESSMENT

4.1 Structure of Assessment Undertaken

50. The structure of my assessment includes the six cross-cutting topics and, for each topic, I explain the assessment approach undertaken and the documents that I have sampled in depth during GDA. This assessment section is therefore structured as follows:

- Nuclear safety principles
- Safety case development
- Commitments management
- Safety case requirements management
- Approach to operating rules
- OPEX arrangements

51. In addition, I have included a section for assessment of the overall demonstration that, in relation to the topics assessed, relevant risks have been reduced to ALARP, and a further section on safety case consolidation. In the safety case consolidation section, I consider whether all the safety case information presented to me in GDA for each topic has been adequately consolidated into the final version of the PCSR and supporting documents.

52. All six cross-cutting topics covered in this report are broad topics and therefore the sub-sections below have been subdivided as appropriate. Furthermore, in several of the topics I reference out to other GDA Step 4 assessment reports where specific areas of assessment have taken place.

53. In sub-section 4.10, I have summarised the standards, guidance and RGP that I have used in my assessment and provided an overarching view on how those are met for each technical topic.

4.2 Nuclear Safety Principles

4.2.1 Assessment

54. ONR expects (Ref. 40) that the safety case head document, the PCSR, “will identify and describe the nuclear safety principles and criteria used in the design”.

55. Chapter 4 of the PCSR, ‘General Safety and Design Principles’ (Ref. 5) contains the NSPs used in the design of the UK HPR1000. Security and environmental principles are described in the GSR and the PCER respectively and they are not part of my assessment. The NSPs are also described in the RP’s ‘General Safety Requirements’ document (Ref. 11). This report contains the same information as Chapter 4 of the PCSR plus further requirements on autonomy and protection against external and internal hazards. It should be noted that the RP considers the general safety and design principles to be general requirements, hence the similarities between both documents. The RP differentiates between general and specific requirements. The RP considers general requirements as those originated from laws, regulations or codes and standards. This is explained in detail in sub-section 4.5, but in the context of NSPs, it is important to understand the term general requirement.

56. My assessment of the RP’s nuclear safety principles has included Chapter 4 of the PCSR, the ‘General Safety Requirements’ report, a detailed comparison of the RP’s NSPs against ONR’s SAPs (Ref. 2) and the review of the nuclear safety principles route map provided by the RP as a response to my RQs (Ref. 12).

57. I carried out my assessment on PCSR version 1 (Ref. 5) and checked the final version of the PCSR (version 2) (Ref. 41) to ensure that the outcome of my assessment did not change.

58. I considered all SAPs in the detailed comparison between the UK HPR1000 NSPs and the SAPs that I undertook as part of my assessment. I also considered international standards and guidance, such as IAEA 'Fundamental Safety Principles' (Ref. 28), 'Safety of Nuclear Power Plants: Design' (Ref. 29), 'Safety Classification of Structures, Systems and Components in Nuclear Power Plants' (Ref. 32), and 'Deterministic Safety Analysis for Nuclear Power Plants Specific Safety Guide' (Ref. 33), and WENRA 'Safety of New Nuclear Power Plant Designs' (Ref. 35) and 'Safety Reference Levels for Existing Reactors 2020' (Ref. 36). I also considered UK legislation, 'Health and Safety at Work etc. Act 1974' (Ref. 42), and ONR's internal guidance, GDA technical guidance ONR-GDA-GD-007 (Ref. 40).

Comparison Against ONR's SAPs

59. Chapter 4 of the PCSR (Ref. 5) states that the fundamental safety objective "the generic UK HPR1000 could be constructed, operated, and decommissioned in the UK on a site bounded by the generic site envelope in a way that is safe, secure and that protects people and the environment" is based on the IAEA fundamental safety principles. To underpin the fundamental safety objective, the RP developed the NSPs based on international good practice with consideration of UK context.

60. In order to assess the RP's NSPs in Chapter 4 (Ref. 5),I carried out a detailed comparison between those and ONR's SAPs. The bullet points below describe the RP's NSPs as presented in Chapter 4 of the PCSR together with the comparison / alignment against ONR's SAPs:

- Reducing the risks to ALARP – This is aligned with the legal duty to reduce risk so far as is reasonably practicable (SFAIRP), since SFAIRP and ALARP are interchangeable in guidance. I consider this RP's principle to be aligned with ONR's Fundamental Principles FP.4 to FP.6 and FP.8
- I consider that the radiation safety requirements are aligned with ONR's Numerical Targets.
- Defence in Depth (DiD) – I consider this RP's principle to be aligned with international standards and ONR's SAP EKP.3
- Safety analysis covers deterministic safety analysis (Design Basis Conditions (DBC) and Design Extension Conditions (DEC)) and Probabilistic Safety Analysis (PSA) – This section provides the definition of DBC and DEC as well as explaining the objective of PSA. I consider this to be aligned with the fault analysis SAPs FA.1 to FA.3 and PSA SAPs FA.10, FA.12 and FA.14.
- Principles for identification, decomposition, and application of safety functions – This section provides an overview of the three fundamental safety functions (control of reactivity, removal of heat and confinement); their decomposition into lower level safety functions and the application of safety functions to safety measures. I consider that this section is aligned with IAEA SSR-2/1 (Ref. 29) and with the safety systems SAP ESS.3.
- Categorisation of safety functions and classification of Structures, Systems and Components (SSCs) – This section provides extensive guidance on these matters and I consider it to be aligned with ONR's SAPs 'Safety classification and standards', mainly SAPs ECS.1 and ECS.2.
- Engineering substantiation principles – This section includes hierarchy of risk reduction to the design, single failure criterion and redundancy, independence, diversity, human factors, ageing and degradation, and EMIT. I consider these principles to be aligned with ONR's SAPs:

- Key principles EKP series
- Design for reliability EDR series
- Equipment qualification SAP EQU.1
- Maintenance, inspection and testing EMT series
- Safety systems SAPs ESS.10 to ESS.13
- Human factors SAPs EHF.1 to EHF.7 and EHF.10
- Ageing and degradation EAD series

- Applicable codes and standards – This section covers the selection of codes and standards in accordance with the safety classification. I consider this to be aligned with ONR's SAP ECS.3.

61. The General Safety Requirements report (Ref. 11) contains the same information as Chapter 4 of the PCSR plus two extra general requirements under engineering design requirements (autonomy and other requirements) and a further requirement on protection against internal and external hazards. I consider that there is alignment with some of ONR's external and internal hazards SAPs (EHA.1 and EHA.19) and some of the essential services SAPs like EES.1.

62. Based on the above detailed comparison, I judge that the NSPs in Chapter 4 provide the key high-level principles needed for a generic PCSR.

63. However, my assessment also highlighted that whilst there was alignment between some ONR's SAPs and the RP's NSPs, some of ONR's SAPs did not seem to be covered by the RP's NSPs. Although the RP's NSPs do not need to replicate the SAPs, and also, some SAPs are not relevant for GDA, like the siting SAPs, I expected the RP's NSPs to include aspects like the development of fit-for-purpose safety case documentation.

64. I raised RQ-UKHPR1000-1111 (Ref. 12) to clarify if there were NSPs for those areas and also for technical disciplines that were not reflected in Chapter 4 of the PCSR or in the General Safety Requirements report, like Decommissioning. The RP explained that each area / technical discipline in UK HPR1000 had developed its own design principles in accordance with the general safety and design principles and applicable codes and standards. The RP did not provide further design principles, instead examples of general requirements for a limited number of disciplines were provided and those ranged from international codes and standards to RP's submissions. The information presented was limited and whilst it provided visibility of the general requirements, I could not find discipline specific NSPs.

65. In order to understand the totality of the design principles for each technical discipline or technical area, such as, safety case, I raised a further RQ, RQ-UKHPR1000-1295 (Ref. 12). Within this RQ, I requested a road map stating the principle and the safety case sections that identify the principle. The RP's response was comprehensive and provided aspects of principles by technical discipline (e.g., Chemistry, Electrical Engineering) or area (e.g., safety case) with links to the safety case or to international standards and guidance. I sampled the information in the road map, and I found the following:

- The RP does not have specific principles for developing a fit-for-purpose safety case documentation. The information provided in the road map signposted to sections in the 'Safety Case Development Manual' (SCDM) (Ref. 37) that repeated the principles in Chapter 4 of the PCSR and referred to ONR's safety case SAPs. The SCDM did not identify any RP's principles for developing safety case documentation.

- For some disciplines, like Fuel and Core or Severe Accident Analysis, the road map referred to IAEA standards, guides and TECDOCs. I consider those to be RGP, but the RP's NSPs (Ref. 5, Ref. 11) do not include discipline specific principles.
- The RP does not have specific principles for pressure systems, containment, ventilation, or use of computer codes. The information in the road map signposted to design standards like RCC-M, ISO or IAEA standards. As before, I consider those to be RGP, but the RP's NSPs do not include pressure systems, containment, ventilation or use of computer codes.
- For the majority of the disciplines, for example, Decommissioning, Chemistry, Electrical Engineering or C&I the road map referred to the RP's design documents. In some cases, like Electrical Engineering and Decommissioning, the road map identified functional and general requirements. In others, like C&I, the road map only referred to sections of reports that provided an overview of specific technical areas with no reference to principles or requirements. I do not consider those to be NSPs, as they are not presented as such in the safety case.

66. I consider that the RP's road map provided clarity on general requirements specific to some technical disciplines, like Decommissioning, but it did not provide further NSPs. General requirements are explained in more detail in sub-section 4.5 of this report.

67. I understand the RP's approach, in terms of considering the NSPs in Chapter 4 of the PCSR as general requirements, but I do not consider general requirements placed in different documents within the safety case (tier 2 and 3 documents) to constitute NSPs for the technical disciplines. Therefore, I judge that the information in the road map confirms that there are not further principles other than the ones in Chapter 4 of the PCSR and the 'General Safety Requirements' report (Ref. 11).

68. Overall, I consider that the NSPs in Chapter 4 are sufficient to support the generic safety case as they cover the key nuclear safety principles, such as ALARP, fundamental principles, key engineering principles and numerical targets, also they are aligned with international RGP. However, my assessment identified that there are not NSPs for specific areas, such as safety case development, or discipline specific NSPs with some exceptions such as protection against external hazards and internal hazards, but those are not covered in Chapter 4. Therefore, I judge that whilst the RP's NSPs are sufficient for GDA, those areas identified in my assessment should be addressed by the licensee when developing its own NSPs. I consider this matter to be significant enough to raise the following Assessment Finding:

AF-UKHPR1000-0106 – The licensee shall develop nuclear safety principles to underpin all aspects of the design and the lifecycle of the nuclear facility. These should include resolving the shortfalls identified during GDA.

69. It should be noted that Bradwell Power Generation Company Limited (BRB) has developed its own NSPs to underpin the design and life cycle of the UK HPR1000 based nuclear power plant that it is proposing to build at Bradwell-on Sea, Essex. Although assessing the BRB NSPs was outside the scope of GDA I have observed that BRB has developed further and expanded the RP's NSPs.

70. I have checked Chapter 4 in the final version of the PCSR (Ref. 41), and the conclusions of my assessment remain the same.

4.2.2 Strengths

71. Following my assessment of the UK HPR1000 general safety and design principles, I have identified the following strengths:

- The RP has developed its own general safety and design principles, in Chapter 4 of the PCSR, which are aligned with RGP and I consider them to be sufficient for GDA.

4.2.3 Outcomes

72. The outcome of my assessment of the UK HPR1000 general safety and design principles is as follows:

- Whilst the RP's NSPs provide high level principles, I have identified that the principles should be developed further to include all lifecycle aspects of a nuclear power station and resolve the shortfalls identified by my assessment. I have raised an Assessment Finding for the licensee to address this.

4.2.4 Conclusion

73. Based on the outcome of my assessment, I have concluded that the UK HPR1000 general safety and design principles are adequate for the purposes of GDA.

74. I have identified a shortfall, for the licensee to address, related to the scope of the NSPs. This is not significant enough to undermine my confidence in the overall adequacy of the generic UK HPR1000 design and safety case, but it is significant enough to warrant ONR's tracking to resolution during the site-specific stages. This is captured as an Assessment Finding.

75. Overall, I am satisfied that at high-level the RP's NSPs are compliant with international RGP (Ref. 28, Ref. 29, Ref. 33, Ref. 32, Ref. 35, Ref. 36) and meet the intent of ONR's SAPs.

4.3 Safety Case Development

76. For the development of the generic UK HPR1000 safety case, the RP developed and implemented a number of tools which are described and assessed below. The majority of those tools also covered the security case, and, in those instances, I make reference to the GSR and the security case.

4.3.1 Assessment

77. ONR expects a GDA RP to establish and deploy suitable means to deliver, in a timely manner, a good quality and comprehensive safety case, which has been subject to appropriate oversight by individuals / functions with authority, expertise and clear vision for what the safety case is trying to achieve. Early in GDA, ONR identified shortfalls in the RP's arrangements to develop the safety case for UK HPR1000, which resulted in ONR raising 'RO-UKHPR1000-0004 – Development of a Suitable and Sufficient Safety Case' (Ref. 9). Actions 1 – 3 of RO-UKHPR1000-0004 requested the RP to implement an adequate safety case development strategy, a delivery programme and the organisational development to support the safety case development strategy.

78. My assessment of the generic UK HPR1000 safety case development has included:

- the RP's responses to RO-UKHPR1000-0004 Actions 1 to 3;
- the RP's implementation of its safety case development strategy;

- the RP's progress in the development of the generic safety case for UK HPR1000 via a project-wide (regulatory) safety case 'health check'; and
- the regulatory oversight of the RP's safety case consolidation.

79. The key SAPs applied within my assessment of the safety case development were SAPs SC.1, SC.2, SC.4, SC.7 and SC.8 and the associated TAGs, NS-TAST-GD-005, 'Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable)' (Ref. 23) and, NS-TAST-GD-051, 'The Purpose, Scope and Content of Safety Cases' (Ref. 27).

4.3.1.1 Safety Case Development Strategy

80. RO-UKHPR1000-0004 was raised by ONR in September 2018 to address several potential shortfalls in the processes and controls being applied by the RP to develop the generic safety case for UK HPR1000. Actions 1 to 3 deal with the strategy, programme, and organisational aspects of producing an adequate generic safety case during GDA. In response to RO-UKHPR1000-0004 Actions 1 to 3 the RP developed the following arrangements (noting that we briefly reported about some of them in the GDA Step 3 Summary Report (Ref. 43)):

- 'Safety Case Development Strategy' report (Ref. 13). This report sets out the safety case development strategy, approach and arrangements required to manage the interfaces between PCSR, PCER and GSR submissions (collectively known as the Safety, Security and Environmental Report (SSER)). It also discusses the overall design process and the link to safety case development with expectations on the 'golden thread' of safety case information and requirements. The strategy report sets out the overarching hierarchy of strategy documents and describes their relationship.
- PCSR and GSR production strategy reports. Each technical discipline has its own production strategy report. The main purpose of the strategy reports is to provide guidance to the safety case authors. The strategy reports also demonstrate that there is a suitable and sufficient suite of safety case documents to demonstrate that the safety case fundamental objective and claims are met and underpinned by sufficient evidence. The production strategies provide traceability of the arguments and evidence through the safety and security cases.
- A procedure (Ref. 44) describing an Integrated Delivery Tool (IDT) and its use in developing the Integrated Delivery Plan (IDP), the Master Document Submission List (MDSL), the Document List (DL) and the 'totality of safety case list'.
- UK HPR1000 GDA 'Safety Case Development Manual' (SCDM) (Ref. 37). This constitutes a resource for safety case authors on how to write a safety case that is fit-for-purpose in the UK context, meeting the expectations outlined in the 'Safety Case Development Strategy' report (Ref. 13). The SCDM has been updated to include improvements such as the safety case requirements management process.

81. I consider that the 'Safety Case Development Strategy' report (Ref. 13) provided a good overview of the RP's arrangements, pulling together information that had previously been incomplete or inconsistent into a useful overarching document. I consider the 'Safety Case Development Strategy' (Ref. 13) to be aligned with SAP SC.1, as it describes the safety case production process.

82. The production strategy reports provided a more detailed description of how the safety case for each technical discipline, and the security case, would evolve over the course of GDA and beyond. They provided information on the document hierarchy, document route map, as well as the objective, scope and content of planned documentation in

the technical discipline to fulfil the safety case for that topic throughout GDA Steps 3 and 4. They were critical documents for ONR's assessment team, as they were the first formal articulation of the detailed structure of the safety case across all assessment areas. Before this point ONR was unsighted on what documents the RP intended to submit during GDA and how they would articulate the 'golden thread' that links the safety analysis to the design of the plant and its operational control measures. The production strategy reports were updated throughout Step 4 of the GDA to reflect the safety case development, for example, the latest update included a summary of the safety case consolidation in the different technical disciplines. I consider the production strategy reports to be aligned with SAP SC.2, in particular as they describe the different levels and types of documentation within the safety case for a particular discipline.

83. The main issue that I identified from my review of the strategy documents was that they did not describe how the structure of the safety case would allow the golden thread to be adequately demonstrated. In response to my finding, the 'Safety Case Development Strategy' report was updated with a high-level description of how the various submissions would fit within the RP's understanding of the golden thread, which I consider to be a useful addition, and aligned with SAP SC.4 (safety case characteristics).

84. Overall, I consider that the documented strategy broadly met ONR's expectations with regard to setting out how the safety and security cases were developed during GDA. It served its function to set out the RP's vision and approach to the safety and security cases and allowed a shared understanding of the safety and security cases by both the RP and ONR. The adoption and implementation of the safety case development strategy and the discipline specific production strategy reports led to improvements in the quality of the safety and security cases; progress was monitored by ONR during Step 4 of the GDA, see sub-section 4.3.1.4.

4.3.1.2 Safety Case Delivery Programme

85. The RP developed the IDT, which is a database system used to consolidate the various document trackers that had preceded it. The IDP was intended to facilitate the monitoring of the production, review and submission dates of GDA documents at the various tiers of safety case documentation. The IDT also provided live outputs in different formats for specific purposes, including:

- The IDP, which was a live list compiling the totality of the planned GDA safety and security case submissions. The IDP presented production and review dates as well as the agreed delivery dates for submission to regulators.
- The MDSL, which is a live list of the totality of the GDA submissions at tiers 1 to 3. The MDSL is a key RP's reference as it is one of the documents listed in the DAC if/when granted by ONR to unambiguously define the basis of what has been included within the scope of GDA and against which the DAC is granted.
- The DL, which was the live list of the totality of documents submitted to the regulators during GDA, including those sent for information purposes only, as well as responses to RQs, letters, etc.
- The totality of safety case list included all the submitted and planned safety case documentation plus the list of documents not specifically intended for submission (but which remained available for sampling by the regulators).

86. Visibility of the totality of safety case list was a key development for the project as it enabled ONR to understand the wealth of information that the RP held (much of it originating from Fangchenggang NPP Unit 3, the UK HPR1000 reference plant) that was relevant to, and underpinned, the safety case. Visibility of this information greatly enhanced ONR's ability to identify documents that were sampled during Step 4 of the

GDA. It also enhanced the efficiency of the project by facilitating targeted sampling of supporting documentation containing arguments and evidence.

87. The IDP and the MDSL were shared with ONR on a monthly basis. I consider that the IDP facilitated a better shared understanding of the status of work on the safety and security cases. It also allowed each assessment topic to identify what information it would receive, when it would receive it, and any threats to delivery.

88. The IDP was effectively used in the later stages of Step 4 of the GDA to provide visibility of the RP's safety case consolidation plans and progress.

89. Based on the above, I have concluded that the RP provided a programme for delivery of the generic UK HPR1000 safety case with the tools and sufficient detail to demonstrate the feasibility of the safety case strategy.

4.3.1.3 Safety Case Development Organisation

90. To ensure the adequacy of the organisation to produce the generic UK HPR1000 safety case throughout GDA, the RP developed and implemented:

- Organisational arrangements with specific roles such as CGN's safety case manager and GNSL's safety case project correspondent (Ref. 45).
- A range of procedures that set out how GNSL, CGN and EDF would manage their internal organisations to deliver the generic UK HPR1000 safety case. Those procedures included:
  - 'Organisation and Operation Rules of UK HPR1000 GDA Project'. (Ref. 46).
  - Arrangements for ensuring that Suitably Qualified and Experienced Personnel (SQEP) would undertake the roles, such as 'Suitably Trained, Competent & Experienced Personnel – a Framework for GDA' (Ref. 47) or 'Position Training Guideline and Management Rules on Authorisation and Job Taking' (Ref. 48).
  - A procedure for controlling the safety case production, review and approval process 'Control of Service Provider Technical Work Procedure' (Ref. 49).
- Specific training on UK context topics such as ALARP, OPEX, safety case traceability and requirements management (Ref. 50, Ref. 51).
- The SCDM (Ref. 37) that consolidates all the training and guidance given to the safety case authors.

91. The RP nominated as safety case manager an experienced officer at CGN with authority and influence who, throughout the remainder of GDA, has ensured the effective implementation of the RP's generic UK HPR1000 safety case strategy and programme.

92. The adequacy of the organisational arrangements was sampled in several workshops working jointly with ONR's MSQA lead inspector (Ref. 50, Ref. 52, Ref. 53) and those arrangements were considered satisfactory for GDA.

93. Based on the above evidence, I judge that the RP put in place an adequate organisation and arrangements to produce and develop the generic UK HPR1000 safety case. The arrangements developed by the RP to control the safety case production and maintenance were aligned with the expectations regarding safety case production (SAP SC.1), safety case maintenance (SAP SC.7) and safety case

ownership (SAP SC.8). I consider that the advice given to safety case authors in the SCDM was aligned with the characteristic expected from a safety case (SAP SC.4).

4.3.1.4 Implementation of Safety Case Strategy and Safety Case Health Check

94. During Step 3 and the beginning of Step 4 of the GDA, the RP made progress implementing the safety case strategy. However, ONR's GDA assessment team continued to highlight issues with the quality in terms of 'assessability' of the safety case documentation, and, in particular, difficulties in following the 'golden thread' within the safety case.

95. At the beginning of Step 4 of the GDA, ONR developed what we generically called safety case health check (Ref. 54) to consolidate ONR's overall project view on the quality of the safety and security case submissions, which were the basis for the GDA Step 4 assessments. These included the PCSR version 1, GSR version 1, supporting references as listed in the version of the MDSL live at that time, and consideration of the RP's responses to RQs and ROs, which have been eventually formally integrated into the safety case documentation.

96. ONR assessed the safety case against eighteen suitability criteria set out in a bespoke template. The criteria and questions were based on ONR's expectations for a safety case, as given in NS-TAST-GD-051, 'The purpose, content and scope of safety cases' (Ref. 27). ONR also assessed the security case but this was done pragmatically against the safety case-based criteria and the question set.

97. The safety case health check highlighted four areas for improvement:

- Traceability – Most chapters of the PCSR did not present sufficiently clear and coherent trails from the safety claims (assertions), through the arguments (reasoning) to the evidence that supports the conclusions – 'the golden thread'. Also, the link to the fault and hazards schedules was not always clear in the safety case chapters nor was the categorisation of safety functions and classification of SSCs clear in the safety case.
- Assumptions and requirements – The safety case chapters did not always clearly identify the assumptions, requirements or limits and conditions, which are to be transferred into the construction, operating and decommissioning regimes.
- ALARP – The chapters of the PCSR did not always demonstrate that risks were ALARP, nor identified any actions required to manage risks ALARP in the future.
- Evidence and level of detail – Most chapters of the PCSR lacked suitable and sufficient evidence to fully support the safety case claims and arguments. The key aspects of the safety case were not always sufficiently detailed, clear and justified.

98. The RP implemented a number of actions to improve on the above areas. In terms of traceability, the RP provided further training to all safety case authors and employed UK suppliers to support the safety case development across multiple topic areas. The traceability through the safety case was followed by ONR in subsequent 'project health checks', where the majority of ONR's inspectors reported improvements in this area. In addition, the RP further improved the traceability in the SSER by employing a UK Technical Support Contractor (TSC) to carry out independent checks of the SSER version 2 draft 1. At individual technical level, the traceability through the safety case is reported in the discipline specific Step 4 assessment reports (Ref. 3).

99. The arrangements implemented by the RP to improve the traceability of assumptions and requirements are discussed in detail in sub-section 4.5 of this report.

100. In order to improve on the ALARP demonstration, the RP employed UK TSCs to review several topic specific ALARP demonstration reports and, also, the RP enhanced the 'Holistic ALARP Demonstration Report' (Ref. 55). I reviewed this report and raised several RQs (Ref. 12) asking for further information. The RP addressed all my queries in the latest revision of the report. I consider that the 'Holistic ALARP Demonstration Report' (Ref. 55) is aligned with ONR's NS-TAST-GD-005, 'Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable)' (Ref. 23). Note that ONR's overview of the RP's overall demonstration that the risk associated with the generic UK HPR1000 design is ALARP is covered in the Step 4 summary report (Ref. 4).

101. I followed the improvements on the ALARP demonstration through the safety case meetings with the RP and sought feedback from the ONR assessment team. As a result of the improvements made by the RP, ONR's subsequent project health checks showed that the majority of our inspectors reported improvements in this area. ONR's assessment of the ALARP demonstration for each technical topic can be found in the individual topic reports and the overall ALARP position for the UK HPR1000 is reported in the Step 4 summary report (Ref. 4).

102. In terms of the shortfalls on the evidence and level of detail provided in the safety case, the RP enhanced the training to safety case authors. However, the main influence to address this shortfall was via the interactions with ONR's inspectors which provided further clarity to the RP on the level of evidence required. Many of the identified shortfalls were formally captured by the RP as commitments or Forward Action Plans (FAPs) and those have now been addressed in the latest version of the safety case. The lack of evidence or level of detail was followed up by ONR in subsequent project health checks, where the majority of our inspectors reported improvements in this area. At a technical level, the quality of the evidence and the level of detail within the safety case is reported in the discipline specific Step 4 assessment reports (Ref. 4).

103. In summary, after developing the safety case strategy and a programme for delivering the safety case, ONR assessed the PCSR version 1, GSR version 1, supporting references and the RP's responses to RQs and ROs against the characteristics of a safety case (SAPs SC.2 and SC.4 and ONR's guidance (Ref. 23)) and found a number of shortfalls. These shortfalls were not technical gaps, but gaps in the implementation of the safety case strategy, in terms of safety case characteristics. The RP took several actions to address those shortfalls and those actions improved the safety case and addressed the gaps. Based on the above, I am satisfied with the RP's implementation of its safety case strategy.

4.3.1.5 Safety Case Consolidation

104. The RP's safety case consolidation is part of its safety case development and is a key activity to ensure that the safety case reflects all the work carried out in GDA. The safety case consolidation is the formal incorporation of design modifications, safety case commitments, FAPs, and information provided in RQs and ROs, into the safety case.

105. The work associated with the safety case consolidation is significant, and so I engaged early with the RP to explain ONR's expectation in this area (Ref. 1). As a result of those engagements, the RP understood its importance and developed a safety case consolidation strategy (Ref. 56) which also included the security case. I reviewed the safety case consolidation strategy and had a number of queries, which I compiled in RQ-UKHPR1000-1490 (Ref. 12). My queries related to the RP's plans to provide visibility of the consolidated submissions and how it intended to consolidate RQs' responses into the safety case documentation. The safety case meetings (Ref. 57)

(Ref. 58) and the RQ (Ref. 12) provided the vehicle to clarify and resolve those matters. The matter of visibility was resolved through the production strategies, discussed earlier, and the IDP. In those strategies the RP provided visibility of the consolidated submissions at a discipline level, including security; at a project level the IDP was used as a vehicle to inform ONR of the timescales for the consolidated submissions. The consolidation of RQs' responses was resolved through the production strategies and engagements with ONR's inspectors to understand our expectations. This was reinforced by the RP's internal review of a significant sample of RQs' responses to determine if those should be formally included in the safety case.

106. With the support of the MSQA inspector and the Environmental Agency, I sampled the implementation of the safety case consolidation strategy during a workshop with the RP (Ref. 53). During this workshop, the RP presented its arrangements to identify the documents that needed updating. The information presented and the sampling carried out during the workshop provided visibility of the steps taken by the RP to ensure an adequate safety case consolidation. The RP's consolidation work was supported by a number of quality control activities, including independent sampling checks, project reviews, and final confirmatory checks undertaken by the RP's GDA Project Office. During the workshop, the RP presented the outcome of phase 1 of the consolidation work carried out; this highlighted a number of documents, mainly linked to RQs and design modifications, that needed further consolidation. The RP summarised the consolidation process and the results (including security) in the 'Safety Case Consolidation Summary Report' (Ref. 59). I have reviewed this report and the information presented is consistent with the outcome of the workshop (Ref. 53). This report also provides assurance on the internal review carried out by the RP.

107. Although I have referred to safety case consolidation in the previous paragraphs, it is important to note that the security case was also consolidated by the RP in the same way as described above.

108. Although, each technical discipline reports on the consolidation of the safety case in the individual assessment reports (Ref. 4), in terms of strategy and its implementation, I consider that the RP's safety case consolidation strategy is adequate. Also, the safety case workshop provided me with confidence on the level of implementation. I have assessed the safety case consolidation of the six cross-cutting topics covered by this report in sub-section 4.9.

4.3.1.6 PCSR Assessment – Chapter 20 – Safety Case Development

109. The RP updated version 1 of the PCSR to reflect the work undertaken during Step 4 of GDA and provided ONR with an advance copy of the PCSR version 2 (Ref. 6). I reviewed this report and have later checked the final version of the PCSR (Ref. 60) to ensure that the outcome of my assessment remained the same.

110. The RP updated Chapter 20 of the PCSR to reflect the safety case development. I have assessed the update (Ref. 6). The RP has included a new section on safety case consolidation that describes the process and references the Safety Case Consolidation Strategy (Ref. 56). The advance PCSR version 2 included a FAP to incorporate the Safety Case Consolidation Summary report (Ref. 59) and I can confirm that in the final version of the PCSR the FAP has been fulfilled.

111. Chapter 20 of the PCSR mentions the Safety Case Development Strategy (Ref. 13), the production strategies at a topic level, the Safety Case Development Manual (Ref. 37) and the tools to deliver the safety case (IDT, MDSL, DL and the IDP). An overview of the safety case management organisation is also provided as well as the arrangements for the demonstration of risk reduction to ALARP.

112. The overview of the safety case development provided in Chapter 20 of the PCSR covers all the aspects considered in my assessment and provides links to key documents. Therefore, I consider Chapter 20 to provide an adequate overview of the safety case development.

113. I have checked Chapter 20 in the final version of the PCSR (Ref. 60), and I can confirm that the outcome of my assessment remains the same.

4.3.2 Strengths

114. Following my assessment of the generic UK HPR1000 safety case development, I have identified the following strengths:

- The RP developed an adequate Safety Case Strategy and programme.
- The shortfalls identified during ONR's safety case health check were adequately addressed by the RP, demonstrating that there was an adequate organisation in place to deliver the generic UK HPR1000 safety case.
- The RP developed and implemented the safety case consolidation strategy which was supported by a number of quality control activities.
- PCSR Chapter 20 provides an adequate summary of the safety case development with references to the key supporting information.

4.3.3 Outcomes

115. Following my assessment of the generic UK HPR1000 safety case development, I have not identified Assessment Findings in the RP's safety case development arrangements or in the general implementation of those arrangements, however:

- At discipline level, the adequacy of the RP's arguments to justify that risks have been reduced to ALARP is reported in the topic specific Step 4 assessment reports (Ref. 3). The adequacy of the RP's holistic ALARP case is reported in the Step 4 summary report (Ref. 4).
- The adequacy of the traceability and the level of detail within discipline-specific safety case submissions is reported, as appropriate, in the topic specific Step 4 assessment reports (Ref. 3).
- The adequacy of the safety case consolidation in the individual technical disciplines is reported in the topic specific Step 4 assessment reports (Ref. 3).
- My assessment of the RP's safety case requirements management is reported in sub-section 4.5 of this report and there are several Assessment Findings on this area.

4.3.4 Conclusion

116. Based on the outcome of my assessment of the safety case development, I have concluded that the RP established and deployed suitable means to deliver, in a timely manner, a comprehensive generic safety case for UK HPR1000. I am satisfied that relevant expectations derived from SAPs SC.1, SC.2, SC.4, SC.7 and SC.8 and TAGs, NS-TAST-GD-005, 'Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable)' (Ref. 23) and NS-TAST-GD-051, 'The Purpose, Scope and Content of Safety Cases' (Ref. 27) are met.

4.4 Commitments Management

117. In sub-section 4.3, I explained how the RP responded to Actions 1 to 3 of 'RO-UKHPR1000-0004 – Development of a Suitable and Sufficient Safety Case' (Ref. 9). However, there was a further action, Action 4, within this RO that dealt with the

capturing and management of assumptions, requirements and commitments from the generic safety case.

118. This section covers my assessment of the RP's arrangements for capturing, managing, and implementing commitments within the safety case. My assessment of the RP's arrangements for capturing and managing assumptions and requirements from the safety case is described in sub-section 4.5, as those arrangements are different to the commitments management arrangements.

4.4.1 Assessment

119. ONR expects (Ref. 40) the RP "to explain and demonstrate how the requirements, assumptions and commitments in the safety case are captured to ensure that the safety case will be realised in practice in any future new nuclear build project using that design."

120. ONR guidance (Ref. 40) also expects "the RP to put in place, early in GDA, a 'commitment capture log'. This document (database) should provide the means to capture, track implementation in the safety case documentation, and demonstrate closure of, all the commitments made by the RP throughout GDA."

121. My assessment of the RP's arrangements to capture, track and implement commitments has included several workshops to sample the RP's arrangements including the commitment log, the review of the 'Management of Commitments for UK HPR1000 Generic Design Assessment (GDA) Project' , (Ref. 14) and assessing the RP's arrangements for capturing post-GDA commitments. I have not assessed the technical content of the commitments as this is considered at discipline level and reported in the topic assessment reports (Ref. 3), where appropriate.

122. The key SAPs applied within my assessment of commitments management were SAPs SC.1, SC.2 and SC.8 and the associated TAG, NS-TAST-GD-051, 'The Purpose, Scope and Content of Safety Cases' , (Ref. 27) and the GDA technical guidance, ONR-GDA-GD-007 (Ref. 40).

123. The RP's arrangements for managing commitments are described in CGN's procedure GH-40M-020 (Ref. 14) and the GNSL procedure 'Management of Commitments for Safety Case Updates' (Ref. 39). Both documents contain very similar information, but the GNSL procedure (Ref. 39) contains information on GNSL's responsibilities on the process. I consider those documents to be aligned with the expectation in SAP SC.8 regarding the ownership and definition of responsibilities. According to the procedures, the sources of commitments can be RQs, information from meetings or workshops with ONR and FAPs in the SSER or supporting documents. In the RP's arrangements ROs are not a source of commitments, as ROs have their own resolution plan which captures their implementation into the safety case.

124. Once a commitment is identified, it is then captured in the RP's commitment log. It should be noted that the commitment log also includes security commitments. The commitments in the commitment log are classified as GDA commitments, to be closed during GDA, or post-GDA commitments for the licensee to consider and address. The commitment log is the RP's tool to track commitments and it was shared on a monthly basis with ONR. The process for managing GDA commitments has been discussed during the safety case and MSQA Step 4 interactions. Those interactions included workshops with the RP on commitments management, and highlighted several matters that required follow-up and which I brought to the RP's attention:

- The commitment log did not provide traceability on how commitments were incorporated into the safety case. Therefore, commitments were closed without

providing that traceability, and in some cases, commitments were wrongly closed.

- During the identification of a commitment, the RP needs to decide if a commitment is a GDA commitment or a post-GDA commitment. The workshops with the RP highlighted that the RP did not have criteria for identifying post-GDA commitments.
- The post-GDA commitments were only captured in the commitment log, which was a separate document, not referenced from the PCSR or included in the MDSL.

125. The RP addressed all three shortfalls. The lack of traceability was addressed by adding a column that explained the reasons for closing the commitment and signposting to the documents that were modified as a result of the commitment. I consider this to be aligned with SAP SC.2 in terms of providing clarity on the trail from claims through arguments to evidence, in other words the golden thread. This information was added to all commitments made after June 2020, however, during the safety case consolidation a further check was carried out of commitments made before that date.

126. The RP developed criteria for identifying post-GDA commitments which was added to procedure GH-40M-020 (Ref. 14) and to the GNSL procedure (Ref. 39). The commitment log was modified to include the reasoning for considering a commitment as a post-GDA commitment. I reviewed the criteria, and I had several queries (Ref. 12) that the RP addressed.

127. In order to address the final shortfall, the RP captured all post-GDA commitments into a tier 2 document (Ref. 15) that is a reference in the PCSR. I reviewed the 'Post-GDA Commitment List' (Ref. 15) in terms of process and I raised several queries (Ref. 12) that the RP addressed. It was important to capture the 'Post-GDA Commitment List' in the MDSL because the MDSL is one of the documents listed in the DAC if/when granted by ONR and therefore provides traceability to this document. The licensee will have to develop a process for managing the post-GDA commitments and I consider this to be normal business.

128. During the safety case consolidation, the RP reviewed all commitments made from the beginning of Step 4 of the GDA and 10% of the commitment made before Step 4 of the GDA to ensure that they were properly incorporated in the safety case. Those checks showed that all commitments were incorporated in the safety case. I consider that the commitments process and the checks carried out by the RP aligned with the expectations related to the safety case production process, SAP SC.1.

129. Overall, my review of the RPs arrangements for managing commitments highlighted several shortfalls, but those were addressed satisfactory by the RP. I also consider those arrangements to be aligned with ONR's expectations in SAPs SC.1, SC.2 and SC.8 and NS-TAST-GD-051, as the commitment management process improves the safety case golden thread. Therefore, I judge the RP's arrangements for capturing, tracking and implementing commitments into the safety case adequate for GDA. Furthermore, the checks carried out during the safety case consolidation showed that all commitments were consolidated in the safety case, providing me with further confidence in the RP's commitment management process.

PCSR Assessment – Chapter 20 – Commitments Management

130. The RP updated version 1 of the PCSR to reflect the work undertaken during Step 4 of GDA and provided ONR with an advance copy of the PCSR version 2 (Ref. 6). I reviewed this report and have later checked the final version of the PCSR (Ref. 60) to ensure that the outcome of my assessment remained the same.

131. The RP updated Chapter 20 of the PCSR to reflect the commitments management arrangements. I have assessed the update (Ref. 6). The RP included a new section on commitments management that described the process, including the commitment log, references the commitment management procedures (Ref. 14, Ref. 39) and the post-GDA commitments. However, the update did not reference the 'Post-GDA Commitment List' (Ref. 15), I raised this with the RP and a reference to this document was included in the final version of the PCSR Chapter 20 (version 2) (Ref. 60). I am content that the commitments management section provides an overview of the RP's arrangements and refers to key documents such as the RP's procedures and the 'Post-GDA Commitments List'.

4.4.2 Strengths

132. Following my assessment of the UK HPR1000 commitments management, I have identified the following strengths:

- The RP developed an adequate commitments management process.
- Addressing the shortfalls identified regarding the traceability of information in the commitments log, lack of criteria for identifying post-GDA commitments, and traceability of post-GDA commitments through the safety case significantly improved the RP's commitments' management process.
- The RP's review of the consolidation of commitments into the safety case showed that all GDA commitments made during Step 4 were incorporated into the safety case, providing confidence in the commitments management process.
- The RP captured all post-GDA commitment into a single document directly referenced from the PCSR.
- PCSR Chapter 20 provides an adequate summary of the RP's commitments management arrangements with references to the key supporting information.

4.4.3 Outcomes

133. Following my assessment of the UK HPR1000 commitment management, I have not identified Assessment Findings in the RP's arrangements for capturing and managing commitments, or in the general implementation of those arrangements, however:

- The technical adequacy of the commitments is considered at a topic level, and reported, where appropriate, in the topic specific Step 4 assessment reports (Ref. 3).
- The post-GDA commitments are for the licensee to consider.

4.4.4 Conclusion

134. Based on the outcome of my assessment, I have concluded that the RP established adequate arrangements for capturing, managing and implementing commitments during GDA. The RP also captured in a visible way all post-GDA commitments for the licensee to consider. I am satisfied that relevant expectations derived from SAPs SC.1, SC.2 and SC.8, TAG, NS-TAST-GD-051, 'The Purpose, Scope and Content of Safety Cases' and GDA technical guidance, ONR-GDA-GD-007 are met.

4.5 Safety Case Requirements Management

135. As explained in previous sections, ONR raised 'RO-UKHPR1000-0004 – Development of a Suitable and Sufficient Safety Case' (Ref. 9) which has several actions. Action 4 deals specifically with the capturing of assumptions, requirements and commitments from the generic safety case. I have assessed the RP's arrangements for capturing commitments separately, as reported in sub-section 4.4, and so this section focuses

on my assessment of the RP's arrangements for capturing and managing requirements and assumptions in the safety case.

136. The RP's submissions (Ref. 16, Ref. 17) clearly stated that assumptions are considered as requirements, and the same process applies to them. Hence, for the RP, the term 'requirements' includes assumptions.

137. ONR's guidance (Ref. 27) refers to requirements and assumptions as implementable requirements. For brevity, I use the term 'requirements' throughout my assessment, and this should be taken to include both assumptions and requirements as per the definition of 'implementable requirements' in ONR's TAG.

138. The closure note for RO-UKHPR1000-0004 (Ref. 61) contains further information on ONR's assessment of the RP's response to RO-UKHPR1000-0004 Action 4.

4.5.1 Assessment

139. ONR expects (Ref. 40) that the RP puts in place controls and processes to capture and manage safety case requirements to be applied consistently across all aspects of the generic safety case, and to ensure that those requirements can be effectively handed over to a licensee. SAP SC.6 sets the expectation that the safety case should explicitly identify all the important operational and management requirements of the safety case that must be implemented to ensure safety. However, the generic safety case produced during GDA is not complete and will be further developed by a licensee. Therefore, I have limited my assessment to a suitable and sufficient demonstration, as proof of concept, that safety case requirements are appropriately identified and managed by the RP during GDA.

140. My assessment of safety case requirements management is divided into four main parts:

- Requirements management approach – I have assessed the RP's approach, including the main documents that describe the requirements management approach.
- Requirements management scope – I have reviewed the requirements management scope for GDA.
- 'Requirements Management Regulations' (Ref. 17) – I have assessed this procedure that details the purpose, scope and responsibilities associated with requirements management, as well as the process to classify, identify, transfer, record and uniquely code requirements.
- Requirements management examples – I have sampled the detailed design safety case documents that were used by the RP to demonstrate application of its requirements management process for GDA.

141. I have also sampled the requirements management for layouts but to a limited extent. Within my assessment, I have also considered the arrangements for transferring the safety case requirements to a licensee.

142. The MSQA aspects associated with the RP's requirements management have been assessed in the MSQA Step 4 report (Ref. 62).

143. The key SAPs (Ref. 2) applied within my assessment were SAPs SC.2, SC.4, SC.6, ECS.3, ECE.12, ECV.2, ECV.3 and EMT.1. I also used TAGs NS-TAST-GD-051, 'The Purpose, Scope and Content of Safety Cases' (Ref. 27) and NS-TAST-GD-009, 'Examination, Inspection, Maintenance and Testing of Items Important to Safety' (Ref. 23). I have also considered international good practice, such as IAEA 'Commissioning and Operation Specific Safety Requirements' No. SSR-2/2 (Ref. 30) and IAEA

'Leadership and Management for Safety, General Safety Requirements' No. GSR Part 2 (Ref. 31). I have also taken into account WENRA's reference levels (Ref. 36), in particular the principles related to operational requirements. Further details of my assessment can be found in Annex 4.

144. I have also considered the GDA technical guidance (Ref. 40) , which includes details on expectations for safety case implementable requirements.

4.5.1.1 Requirements Management Approach

145. The 'Requirement Management Summary Report' (Ref. 16) summarises the approach adopted by the RP to resolve Action 4 of RO-UKHPR1000-0004. This report together with the RP's requirements management procedure (Ref. 17) document the RP's requirements management arrangements. Importantly, this report also provides the RP's justification for the adequacy of the approach adopted for GDA and summarises the development of this through gap analysis and subsequent optioneering. I assessed this report (Ref. 16) and provided a significant number of comments requesting additional information or clarification through RQs (Ref. 12). The RP's 'Requirement Management Summary Report' was updated as a result of my RQs and it currently has a number of appendices that provide the 'route map' to the examples assessed in sub-section 4.5.1.4 and Annex 4.

146. The RP has an existing requirement management process (Ref. 63) which is CGN's process used in its domestic projects, and so this existing process represented the starting point for UK HPR1000. This approach is embedded within CGN's normal design process. This is a standard approach to design iteration, as part of controlling the design reference and substantiating the engineering and operational design.

147. As part of this, CGN differentiates between general and specific requirements. The former requirements are derived from aspects that apply to multiple topics and areas, such as legal requirements or the RP's NSPs described in sub-section 4.2 of this report. Other types of general requirements are the codes and standards or the general site layout. The specific requirements are derived at the topic level as part of implementing the design process; namely, these are derived from the safety case and include, for example, technical data, functional requirements (which include safety functions), performance requirements, reliability requirements and layout interfaces. The RP views all the requirements as 'design inputs', and these are recorded within separate internal and external databases. The databases are used to control the design inputs and ensure consistency throughout the design process.

148. It is clear from the RP's existing requirement management process (Ref. 63) and from interactions with the RP on this matter, including several MSQA workshops, that CGN relies heavily on its design process and databases to ensure effective requirement management. The RP commissioned an independent review (and gap analysis) (Ref. 64) of its arrangements that highlighted an important gap in the ability to directly apply the CGN approach to UK HPR1000 for GDA. This is summarised as "…the lack of a capability to uniquely follow / manage the life of a requirement in both a forwards and backwards direction…" which was considered to result in a risk that "…it would potentially be difficult for them [the future owners and operators of the plant] to trace the requirements and to understand the design requirements". Based upon my understanding of CGN's approach to requirements management, I agree with this conclusion.

149. Subsequently, the RP carried out optioneering to identify possible solutions to overcome this gap (Ref. 64). I consider that a reasonable range of potential solutions were considered, and the methodology was fit for purpose.

150. The chosen option implemented by the RP builds upon the CGN approach. It is still based around the existing design process but implements a unique coding system to enable tracing of requirements through the safety case. As well as the coding system, the RP developed several schedules: fault, confinement, hazards, duty and engineering schedules that provide a summary of the requirements and links to the safety case. The coding is applied to the design and operational documents such as Safety Functional Requirements Reports (SFRR), System Design Manuals (SDM), operation procedures, civil engineering design reports, etc.

151. In order to understand the RP's process, it is important to also understand its limitations. In terms of coding only a limited sub-set of specific requirements are codified. Whilst I agree with the RP's argument that it is not possible to codify all the requirements, the traceability of non-codified requirements is still very limited. This is explained in more detail in the assessment of the examples, see sub-section 4.5.1.4 and Annex 4.

152. The RP's overall approach is shown in Figure 1 and Figure 2 taken from the 'Requirements Management Summary Report' (Ref. 16).

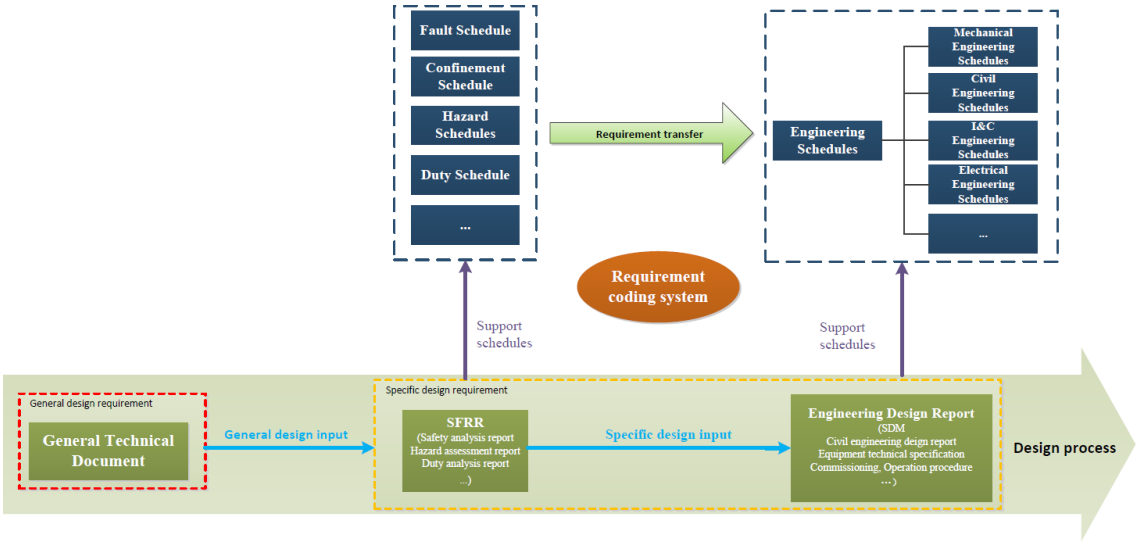

Figure 1: Link between general requirements, schedules, engineering documents and safety functional requirement reports

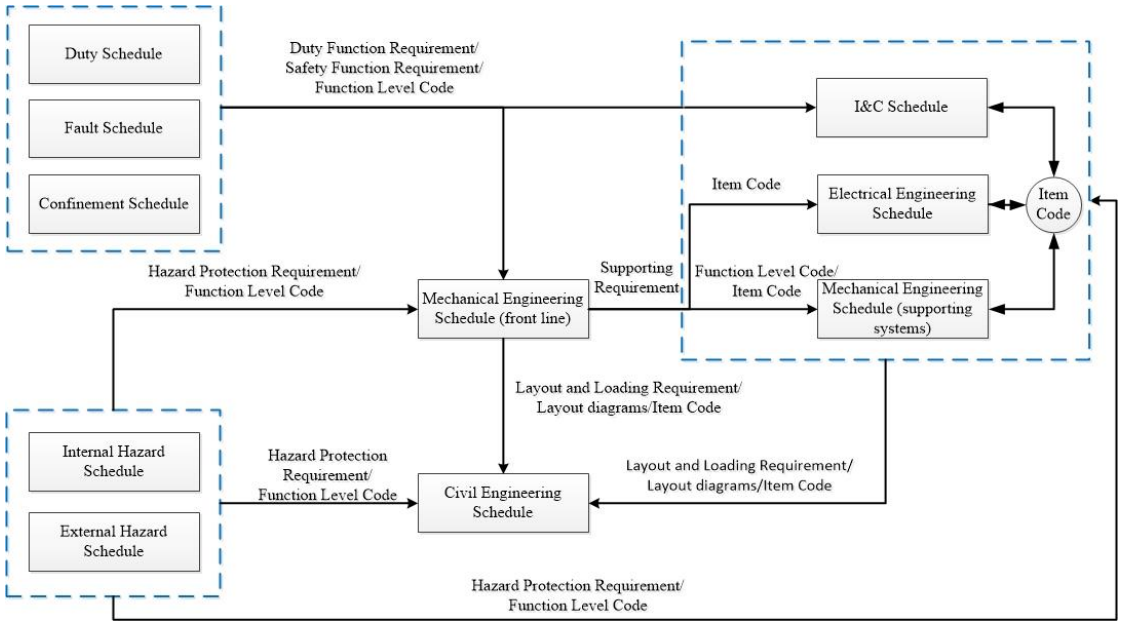

Figure 2: Transfer of requirements between the different schedules

153. The requirement coding system applied by the RP is described in the 'Requirements Management Summary Report' (Ref. 16), and is detailed in the RP's requirements management procedure (Ref. 17). It consists of four fields which represent the system or building code, requirement type, serial number and control mode respectively. Through this coding the RP is able to distinguish the identified requirements, and it in itself provides information to aid the user's understanding of the requirement. At this point it is worth noting the second field regarding requirement type. The RP uses this field to distinguish between the functional requirements associated with faults, severe accidents, confinement, duty and hazards schedules. I assess the adequacy of this approach as part of my sample later in sub-section 4.5.1.4, but in principle, I am content that the application of such a coding system is a reasonable approach to identifying and tracing requirements throughout the safety case. The obvious disadvantage to this approach is that it carries a significant administrative burden and could create errors.

154. The operational aspects of the RP's requirements management are also described in the 'Requirements Management Summary Report' (Ref. 16) and in the RP's requirements management procedure (Ref. 17). Many of the end-documents produced from this process will be site and licensee specific, but the requirements management process, as described earlier, still applies, with the coding and identification flowing through the design process outputs into the operational documentation. This is integrated into the overall design process.

155. The current process only considers the operational requirements derived from the design of SSCs (which the RP contends are themselves derived from the safety analysis). The RP recognises that there will be other operational requirements derived from the Human Factors and PSA but the RP's 'Requirements Management Summary Report' (Ref. 16) and procedure (Ref. 17) do not adequately explain how these are part of the requirements management process. As such, I have considered these further as part of my sample of the RP's implementation examples – see sub-section 4.5.1.4 and Annex 4.

156. Based on the outcome of my assessment of the approach to requirements management proposed by the RP, I conclude that, in principle, using a unique coding

system integrated adequately into the CGN design process is a suitable solution. I judge that the RP has correctly identified the key gap in CGN's arrangements for GDA. It is also evident that the application of the requirements management process to analysis and operational aspects is less well developed than the engineering requirements, and I have factored this gap into my assessment sample of the RP's examples.

4.5.1.2 Requirements Management Scope

157. The requirements management process was applied retrospectively to the RP's generic safety case at a late stage in GDA, and so the scope of application of the requirements management process was limited. The scope was reflected in the schedules and the faults, hazards and the SSCs included on those, so for GDA the scope of schedules was:

- Fault schedule presents the full scope of the DBC and the DEC A.
- Confinement schedule presents the full scope.
- Duty schedule was limited to three system examples: Emergency Feedwater System (ASG [EFWS]), RIS [SIS], and Main Control Room Air Conditioning System (DCL [MCRACS]).
- Internal hazards schedule does not cover the full scope of internal hazard, instead it provides the bounding loading cases. The bounding cases envelop the internal hazards not covered in the schedule.
- External hazards schedule covers the full scope of external hazards for GDA.
- Mechanical engineering schedule (including the equipment qualification schedule) covers the same three systems as the duty schedule plus part of the fuel pool cooling and treatment system (PTR [FPCTS]).
- Civil engineering schedule covers three structures: BFX, internal containment and common raft.
- C&I schedule includes the centralised C&I systems in scope of GDA.
- Electrical engineering schedule – only a template is provided.

158. The scope presented above was the outcome of numerous discussions with the RP at project and discipline level. In my opinion, the above scope is sufficient to demonstrate the controls and processes to capture and manage safety case implementable requirements, which was the expectation for GDA. However, the licensee will need to develop this further and apply the requirements management process to the whole safety case. The RP has captured the further development of the schedules as several post-GDA commitments (Ref. 15). I judge that the licensee will be able to develop the schedules to the full scope as part of its normal design and safety case processes, and so I consider this to be a minor shortfall.

159. A requirements management workshop (Ref. 51) with the RP and my assessment of the RP's requirements management procedure (Ref. 17) highlighted that the scope of this process did not include technical areas such as Spent Fuel Interim Storage or Fuel & Core. This has been acknowledged by the RP (Ref. 17, Ref. 65) and I have captured this shortfall, although I do not mention specific disciplines, in Assessment Finding AF-UKHPR1000-0107 – see sub-section 4.5.1.4.

4.5.1.3 Requirements Management Procedure

160. The 'Requirements Management Regulations' (Ref. 17) describes, at a high level, the requirements management arrangements for UK HPR1000, including the process to classify, identify, transfer, record and uniquely code requirements. This was a new procedure developed in response to RO-UKHPR1000-0004 which is consistent with the 'Requirements Management Summary Report' (Ref. 16). The difference between the two documents is that the Requirements Management Regulations' (Ref. 17)

focuses only on the process and does not provide all the background information and all the detailed examples that the summary report contains (Ref. 16). It should be noted that I refer to the 'Requirements Management Regulations' (Ref. 17) as the RP's requirements management procedure, and that this procedure is supplemented by the 'Requirements Management Summary Report' (Ref. 16).

161. The RP's requirements management procedure (Ref. 17) was updated in response to my assessment. The updates included more visibility on documents containing general requirements relevant to disciplines, for example general requirements on radioactive waste management, a summary of documents containing specific codified requirements, and further examples and explanation on requirements management processes such as function groups. Note that a function group is a set of functions which are associated and often implemented together to achieve one complex function.

162. My assessment also included raising several RQs (Ref. 12) and an inspection (Ref. 51) of the RP's arrangements.

163. I reviewed the RP's requirements management procedure (Ref. 17) and I found that in terms of traceability it provides high level guidance on where requirements are recorded in the safety case. It also provides the links between the schedules and the coding system. The procedure (Ref. 17) covers all the technical disciplines and all the different types of requirements, and so it acts as guidance to the user, rather than an instruction that could be directly applied. This explains some of the difficulties encountered by the RP in applying this to its implementation examples. While the RP has worked to resolve these for the specific examples during GDA, there are still some generic areas in the applications of the procedure that will need to be considered by the licensee. Some of these aspects, which are explained in more detail in Annex 4, need further consideration in terms of additional guidance in the procedure, for example:

- The procedure provides high level advice on how to trace codified requirements through the safety case and lists some of the documents that contain general requirements. However, there is limited information on the traceability of specific requirements that are non-codified, and assumptions in the safety case fall into this category.
- Although the RP's requirements management procedure was updated to include information on function groups, there is still limited guidance in terms of function groups, decomposition of functions and what constitutes a complex function.

164. The RP has acknowledged some of the above findings in its own lessons learnt review (Ref. 65) and has captured the need to implement the lessons learnt as a post-GDA commitment (Ref. 15).

165. Based on my assessment of the RP's requirements management procedure (Ref. 17), I am content that this procedure is consistent with the intent of the approach defined in the 'Requirements Management Summary Report' (Ref. 16) and that it includes useful guidance for its application. I also consider it positive that this forms part of the RP's management system for GDA, which lends confidence that it could be carried forward post-GDA. However, my assessment of the examples below identified several process related shortfalls, including those mentioned above, that need further consideration to ensure that the procedure (Ref. 16) and the summary report (Ref. 17) could be applied consistently by a licensee. I have captured those in Assessment Finding AF-UKHPR1000-0110 below.

166. Nevertheless, for the purpose of GDA, and as part of the RP's demonstration, I am content that this procedure is sufficiently mature.

4.5.1.4 Implementation of Requirements Management Arrangements – Examples

167. The RP's requirements management process discussed in the previous sub-section was applied retrospectively to a sample of systems and structures to demonstrate the suitability of the arrangements developed by the RP. I agreed with the RP that the sample should cover safety significant systems and structures and a wide range of engineering and operational requirement types, and this resulted in the examples in Table 1. The examples were selected to demonstrate the traceability between all schedules developed in GDA (fault, hazards and engineering schedules), through the analysis documents, to the engineering reports. Some examples were chosen to demonstrate traceability of operational requirements.

168. The examples selected are listed in Table 1 and the detailed assessment of those can be found in Annex 4.

Table 1: Examples of systems and structures to demonstrate the implementation of the requirements management process

Number	Example Description
1	The demonstration of full traceability for the full set of engineering and operational requirements and assumptions for the RIS [SIS]
2	The demonstration of full traceability for the operational and engineering requirements and assumptions associated with the cooling functions of the RIS [SIS]
3	The demonstration of full traceability for the operational and engineering requirements and assumptions associated with the clean-up functions of the PTR [FPCTS]
4	The demonstration of full traceability for a set of human factors requirements of the RIS [SIS]
5	The demonstration of full traceability for a set of constructability requirements and assumptions for the Spent Fuel Pool (SFP) liner
6	The demonstration of full traceability for a set of shielding requirements and assumptions for the BFX
7	The demonstration of full traceability for a set of In-service Inspection (ISI) and leak detection requirements and assumptions for the SFP and the In-containment Refuelling Water Storage Tank (IRWST)
8	The demonstration of full traceability for a set of high energy pipe failure requirements and assumptions for the BFX.
9	The demonstration of full traceability for a set of aircraft impact requirements and assumptions for the BFX.
10	The demonstration of full traceability for a set of requirements and assumptions for a Postulated Initiated Event (PIE) that results in a temperature and pressure challenge to the SFP.

169. I have focused my assessment on the identification of the requirements and the traceability of those requirements through the safety case. I have not assessed the

technical adequacy or completeness of the specific requirements, as this is beyond the scope of my assessment. This has been done at the technical disciplines level and reported in their GDA Step 4 assessment reports (Ref. 3), as appropriate.

170. During my assessment I raised several RQs (Ref. 12) and as a result the RP addressed, in the new submissions, some of the gaps identified in my assessment. The RP also updated its requirements management summary report (Ref. 16) and its requirements management procedure (Ref. 17) to address some of the gaps highlighted by my assessment. Further information of my assessment of the examples, including my assessment of the RQ responses, can be found in supporting assessment notes (Ref. 66, Ref. 67, Ref. 68).

171. Technical disciplines like C&I, Fuel & Core Design, Mechanical Engineering and Decommissioning, have assessed the traceability and identification of specific requirements in their technical areas. Their Step 4 assessment reports (Ref. 69, Ref. 70, Ref. 71, Ref. 72) capture any specific shortfalls identified via Assessment Findings. The shortfalls I identified in my assessment are captured in the Assessment Findings below.

172. This sub-section summarises my assessment of the ten examples in Table 1 but for further information on individual examples see Annex 4. In order to provide clarity, I have divided this sub-section into the common aspects that I found during my assessment, which are scope, traceability and identification of requirements, level of detail, and process.

Scope

173. For GDA, the scope of the RP's implementation of its requirements management process was limited to the examples and to the content in the schedules described in sub-section 4.5.1.2. Whilst I was conscious of the limitation in terms of scope and the level of development of some areas of the design, I found scope related aspects that will need to be addressed by the licensee. I summarise those below, but for further information see Annex 4.

174. My assessment of example 1 in Table 1 identified that 'non-typical components' (components which do not directly deliver the safety feature but have impact on the performance of this safety feature) have not been considered in the requirements management process. This is acceptable for GDA as those components will be considered during the detailed design phase. However, this matter needs further considerations by the licensee, and, during the detailed design phase, the requirements management process needs to be applied to all SSCs that fulfil a safety function or can affect the fulfilment of a safety function.

175. I was unable to identify specific human factors requirements on the RIS [SIS] in example 4 of Table 1. While the RP had worked to integrate human factors into the design, this will need to be an area of focus as the requirements management process is applied more widely post-GDA.

176. I was unable to identify specific ISI requirements in example 7 of Table 1, and the RP explained that those will be provided in the detailed design phase. Given that no specific ISI requirements for the IRWST have been provided during GDA, I consider this to be an area that should be prioritised by the licensee for the demonstration of its requirements management process.

177. Finally, non-codified requirements need further development to improve traceability, and aspects related to process and scope. In terms of scope, the licensee needs to

develop robust arrangements for tracing non-codified requirements. I cover the traceability and process aspects in the following sub-sections.

178. I judge that the above shortfalls need to be considered and addressed by the licensee, so I have captured all those aspects as an Assessment Finding.

AF-UKHPR1000-0107 – The licensee shall, in implementing its chosen process to manage requirements identified within the safety case, demonstrate the scope captures all necessary aspects of the safety case. This should include resolving the related shortfalls identified during GDA of:

- Ensuring that all systems, structures and components that are required to fulfil a safety function or can affect the successful fulfilment of a safety function, are subject to the process.
- Ensuring full traceability of the engineering performance requirements for systems, structures and components that fulfil a safety function.
- Demonstrating that the process can be applied to human factors-related requirements, including consideration of the definitions, granularity and clarity of human factors-related requirements, in addition to how it is applied to the underlying analysis.
- Demonstrating that the process can be applied to inspection-related requirements.
- Ensuring the traceability of non-codified requirements through the safety case.

Traceability and Identification of Requirements

179. The main focus of my assessment was to identify the source of the requirements within the safety case and trace those backwards and forwards through the safety case.

180. During my assessment, I identified and traced requirements using the coding system developed by the RP and the suite of documents that contained this coding system, mainly schedules, requirements reports, engineering design reports and operational documents. The RP also makes use of unique item codes that apply to components. These item codes already exist within the RP's design processes and I used them to identify and trace requirements.

181. The traceability of codified requirements throughout the suite of documents that contained the coding system was good. However, in the majority of the examples in Table 1 the source of requirements was a safety analysis document which did not apply the coding system and did not reference the schedules or requirement / engineering design reports. In those cases, I was able to find the source of the requirement, but the traceability was in one direction, as I could not trace the requirement from the safety analysis document to the schedules or engineering documents.

182. I identified a minor shortfall regarding the use of leading zeroes in the coding system, see Annex 4 for further detail.

183. Also, the traceability of non-codified requirements was very limited, and I relied on referencing, engineering identifications (IDs) and my understanding of the structure of the safety case. All the safety case assumptions that I found were non-codified and therefore their traceability through the safety case was not possible without in-depth knowledge of the safety case. Overall, I have not identified any examples where the

RP has treated an assumption as a requirement, in terms of explicit traceability through the safety case.

184. My assessment of example 10 of Table 1 highlighted that existing linkages between schedules need further improvement, including considering new links between schedules. However, in a more general sense, the traceability of requirements in some of the examples was possible because the RP provided 'route maps' within the 'Requirements Management Summary Report' (Ref. 16). I consider this a shortfall, since 'route maps' cannot be provided for all requirements.

185. My assessment of the operational and commissioning aspects highlighted the limited traceability of those, in particular with the use of three-field codes where specific requirements were associated to the same code.

186. I have consolidated all the traceability shortfalls described above into a single Assessment Finding.

AF-UKHPR1000-0108 – The licensee shall, in implementing its chosen process to manage requirements identified within the safety case, demonstrate that it can identify their source and traceability to provide their underpinning within the safety case. This should include resolving the specific shortfalls identified during GDA of:

- Ensuring traceability is bidirectional, from the source of the requirement to the design, analysis or operational documentation and vice versa.
- Providing sufficient references to allow traceability, including for non-codified requirements.
- Improving the linkages between the different documents, including schedules, and in particular where requirements are transferred between documents.
- Ensuring commissioning and operational aspects can be traced sufficiently and in particular to the documents demonstrating fulfilment of each specific safety function.

187. Whilst I have identified several shortfalls regarding traceability of some requirements, in general the identification of requirements in the ten examples in Table 1 was adequate. Also, the traceability of requirements from the hazard's schedules to the civil engineering schedule was adequate and sufficient for GDA.

Level of Detail

188. My assessment of the implementation of the examples highlighted that the definition and granularity of the coding functions and the resulting requirements were not detailed or specific enough. For example, the requirements associated with three-field codes did not provide the granularity needed to identify specific requirements or, for some examples, specific requirements were not provided.

189. Whilst the low granularity is understandable given the level of maturity of the requirements management process, it will be key for the licensee to develop its process to an adequate level of detail. I have raised an Assessment Finding to capture this shortfall.

AF-UKHPR1000-0109 – The licensee shall, in implementing its chosen process to manage requirements identified within the safety case, demonstrate that it is undertaken to an adequate level of detail. The definition and decomposition of functions should be consistent, clear, traceable and to a level of granularity that is sufficient to implement the management of identified requirements.

Requirements Management Process

190. My assessment of the RP's implementation of requirements management identified areas within the existing approach (Ref. 16) (Ref. 17) that need further consideration. Some of those have been mentioned in sub-section 4.5.1.3, like guidance on non-codified requirements. However, there are others like classification and grouping of requirements which are summarised below and explained further in Annex 4:

- I identified inconsistencies in the classification of requirements, mainly on requirements wrongly classified as 'other functional requirements' instead of 'duty functional requirements'. Clarity is needed in the classification of requirements before the process is applied more widely.
- The engineering requirement IDs are a useful tool to trace requirements through the civil engineering safety case but those are not mentioned in the procedure (Ref. 17) and their use should be considered further.
- I identified inconsistencies in the grouping of functional requirements (which I refer to as 'grouping of functions'), lack of clarity and simplifications in the coding system that led to lack of traceability. To address this, further guidance is required in terms of function groups, complex functions and on the use of simplified coding (three-field coding).
- Some of the inconsistencies regarding the grouping of functions relate to mixing active and passive functions within a group. The guidance provided by the RP is limited and sometimes unclear.
- I found several inconsistencies in the safety case documentation, such as the wrong grouping of functional requirements. Whilst these are quality assurance matters, the licensee needs to have adequate verification activities inherent in its process.

191. I consider the requirement management process adequate for GDA, but its implementation has highlighted shortfalls in the process that will need to be addressed by the licensee. I have consolidated those into the Assessment Finding below:

AF-UKHPR1000-0110 – The licensee shall, in implementing its chosen process to manage requirements identified from the safety case, enhance the requirements management process demonstrated during GDA by:

- Providing additional guidance over the interface and overlap between fault, duty and other functional requirements and their definition in terms of the categorisation of the safety functions.
- Providing additional guidance on the grouping of individual functions to ensure traceability, including the use of function groups, complex functions and three-field codes.
- Avoiding the mixing of passive, active, manual and automatic functions in function groups where it is not appropriate to do so.
- Clarifying the use of engineering requirements identifiers and item codes to aid with traceability.
- Including guidance on traceability of non-codified requirements.

- Ensuring that adequate verification activities are included in the process to ensure correctness and alignment across the suite of safety case and design documents.

4.5.1.5 Requirements Management - Layouts

192. The RP's layout requirements management is described in the 'Requirements Management Summary Report' (Ref. 16). The process is implemented through three-dimensional and two-dimensional forms (3D model and drawings) and is described in three steps, which I summarised below:

- Step 1 – Design requirements identification – Generally the requirements identified are general design requirements, such as the conventional health and safety, for example minimum platform width, and equipment requirements like dimensions. This information is collected through the internal interface management system, drawings, 3D model, and reports.
- Step 2 – Implementation of the layout design – The layout requirements are implemented at different depths during the design phases, for example, at GDA design level the layout design is implemented at the general arrangements level, although for some topics such as Internal Hazards further detail is provided. Layout requirements are not codified.
- Step 3 – Review of the layout design outputs and delivery to downstream departments.

193. The implementation of the above process, and in particular the use of the 3D model to identify design requirements, has been considered at the technical specialist level during GDA. Furthermore, there is a cross-cutting topic on layouts that is reported in the Step 4 summary report (Ref. 4).

194. From the perspective of requirements management, the layout requirements are not codified, and the majority are captured in the 3D model. I am satisfied that the RP's approach is adequate in this regard. Also, through sampling and interactions with the RP, I have gained sufficient confidence on the RP's arrangements for capturing requirements in the 3D model, and on the control and checks done in the model (Ref. 73, Ref. 74). Hence, I consider those arrangements to be adequate for GDA. As part of normal business and as the detailed design progresses, I would expect the licensee to continue to demonstrate the adequacy of the layouts' management process at a greater depth during the detailed design phase.

4.5.1.6 Transfer to the Licensee

195. As part of my assessment of the RP's requirements management process and in alignment with ONR's expectations (Ref. 1), I considered how requirements identified in the safety case will be transferred to the licensee to be included in operating rules, technical specifications, commissioning programmes, etc.

196. The RP has developed the requirements management procedures (Ref. 16, Ref. 17) explaining how the safety case requirements are transferred to the operational documentation, and it has also provided a number of examples to illustrate its approach.

197. In my assessment I have sampled how requirements originated in the fault analysis disciplines were transferred to the engineering disciplines with the use of schedules and the coding system. The RP also developed several examples to illustrate how

those requirements feed into the construction, commissioning and operational documents, and I assessed those in detail (see Annex 3).

198. In summary, the schedules and the coding system (including item coding) provide the mechanism to transfer the requirements within the safety case to the operational and commissioning documentation. For example, I have sampled the 'Periodic Test Completeness Note (PTCN)' (Ref. 75), 'System Commissioning Programme' (Ref. 76) and 'EMIT Windows' report (Ref. 77), and the requirements are transferred through schedules and coding. I have also sampled the suitability of the operating rules' arrangements for transfer to a licensee in the approach to operating rules cross-cutting topic, where the RP provided methodologies or high-level approaches to develop those. Furthermore, my assessment has included the construction requirements, which are not codified but are transferred through referencing.

199. Notwithstanding the AFs raised before, I consider that the RP's requirements management process is adequate to identify and transfer requirements in the safety case to a licensee for those to be included in construction, commissioning and operational documents.

4.5.1.7 Summary of Requirements Management Assessment

200. After assessing the RP's requirements management approach and the above examples, I have noted some strengths and weaknesses in the RP's process and the ability to identify and trace requirements through the safety case:

- The RP has developed a suitable process for managing requirements in the UK HPR1000 GDA and has provided a demonstration of its implementation through a number of examples.
- The safety case identifies requirements, certainly the most safety significant ones, and the requirements management process improves the traceability of those requirements. This is aligned with the expectations in SAPs SC.2 and SC.4 in terms of golden thread, and SAP EMT.1 regarding the identification of requirements.
- The RP has developed a procedure (Ref. 17) to document its requirements management process. Whilst this is sufficient for GDA there are a number of areas that need enhancement.
- The definition and granularity of the functions and the resulting requirements, as currently presented, are not detailed or specific enough.
- The scope of application of the requirements management was agreed with the RP to demonstrate the process in GDA; my assessment has identified areas that need further consideration.
- The traceability of requirements is largely achieved in the design documents with the requirements managements coding (functional and item codes) helping significantly with this.
- Tracing of the requirements into the safety analysis documentation is difficult and normally in one direction (from the schedules or engineering design reports to the safety analysis documentation). The coding (functional or item) is not used in these parts of the safety case.
- The treatment of assumptions does not appear to be consistent with the RP's requirements management process. I have not identified any examples where the RP has treated an assumption as a requirement.
- The traceability of non-codified specific requirements needs further consideration, as the current arrangements are limited and insufficient in some cases.
- For GDA, the RP has developed adequate arrangements for managing layouts requirements.

- The RP has adequate arrangements for transferring requirements within the safety case to a licensee to develop construction, commissioning and operational documentation.

201. The RP developed training on the requirements management process for the safety case authors and a transition plan for transferring the requirements management process to the licensee. I have considered those arrangements (Ref. 61) and concluded that they are sufficient for GDA.

4.5.1.8 PCSR Assessment – Chapter 20 – Safety Case Requirements Management

202. The RP updated version 1 of the PCSR to reflect the work undertaken during Step 4 of GDA and provided ONR with an advance copy of the PCSR version 2 (Ref. 6). I reviewed this report and have later checked the final version of the PCSR (Ref. 60) to ensure that the outcome of my assessment remained the same.

203. The RP updated Chapter 20 of the PCSR to reflect the requirements management arrangements. I have assessed the update (Ref. 6). The RP has included a new section on requirements management that describes the process, references the requirements management approach (Ref. 16, Ref. 17) and explains that the application was limited during GDA but will be expanded by a licensee. While the update does not identify the key requirements management gap that was being addressed, nor whether this has been closed, I am content that this new section is appropriate for a high-level document such as the PCSR, and that it is consistent with the information in the RP's requirements management procedure (Ref. 17) and in the 'Requirements Management Summary Report' (Ref. 16).

204. I have checked the requirements management section in the final version of the PCSR (Ref. 60), and I can confirm that the outcome of my assessment remains the same.

4.5.2 Strengths

205. Following my assessment of the RP's requirements management arrangements for the UK HPR1000, I have identified the following strengths:

- The RP has developed a suitable process for managing requirements in the UK HPR1000 GDA and provided a demonstration of its implementation through a number of examples. This is aligned with the expectations in SAPs SC.2, SC.4 and SC.6.
- Whilst the process needs further development, it could be used by the licensee to identify and trace requirements, which was one of the main gaps identified in Step 4.
- The RP documented the requirement management approach in a defined procedure embedded within its management system. While still in need of further development, I consider this procedure to be fundamentally sound.
- The examples selected to demonstrate the process, listed in Table 1, represented a good sample of the breadth and depth of requirements found within the safety case for UK HPR1000, albeit limited by the level of development and detail available during GDA
- PCSR Chapter 20 provides an adequate summary of the RP's requirements management arrangements with references to the key supporting information.

4.5.3 Outcomes

206. Following my assessment of the RP's requirements management arrangements for the UK HPR1000, I have identified that whilst the arrangements are adequate for GDA,

there are shortfalls that must be resolved after GDA by the licensee. I have raised four Assessment Findings to capture those matters which I summarise below:

- The scope of the requirements management arrangements needs to capture all necessary aspects of the safety case.
- The requirements management process should identify the source of the requirements and provide bidirectional traceability through the safety case.
- The level of detail provided in the definition and decomposition of functions needs to be sufficient to trace and manage requirements.
- The requirements management processes should be enhanced to provided further guidance on the aspects highlighted by my assessment, including ensuring adequate verification activities.

207. I also identified two minor shortfalls as discussed in sub-section 4.5.1.

4.5.4 Conclusion

208. Based on the outcome of my assessment I consider that the RP's requirements management arrangements for the UK HPR1000 are adequate for the purposes of GDA. Safety case requirements management was an important area of focus for ONR, as earlier in GDA the RP did not have a process for identifying and tracing requirements backwards and forwards through the safety case that could be transferred to a licensee. The RP developed a suitable process for managing requirements within the safety case and provided a number of examples to demonstrate its implementation. I assessed the RP's requirements management procedures and their application, which demonstrated that the safety case identifies the most safety significant requirements and the process developed improves the traceability of requirements. However, whilst I consider that the RP's requirements management arrangements can be used by a licensee to identify and trace requirements, it needs further development. Therefore, I have identified matters that need to be resolved by the licensee and captured them in four Assessment Findings.

209. Overall, I am satisfied that the requirements management arrangements developed by the RP meet the intent of the relevant ONR's SAPs, TAGs and the international guidance described in sub-section 4.5.1.

4.6 Approach to Operating Rules

210. There is a clear overlap between this assessment and the safety case requirements management assessment covered in sub-section 4.5 of this report. Operating rules are one category of requirements from the safety case, and therefore fall under the scope of the process developed by the RP to respond to RO-UKHPR1000-0004. In this assessment I do not consider aspects that have been already assessed under the scope of RO-UKHPR1000-0004 above.

211. Regarding the definition of operating rules, this term should be interpreted as the operational limits and conditions necessary for nuclear safety derived from the safety case. I have summarised below my assessment of the RP's approach which is explained in greater detail in my assessment note (Ref. 78).

4.6.1 Assessment

212. ONR expects (Ref. 1) the RP to provide "a demonstration that the constructed plant will be capable of being operated within safe limits" and "arrangements for moving the safety case to an operating regime; i.e. the arrangements to ensure that the requirements of, and assumptions in, the safety case have been clearly identified and can readily be captured in: …(f) operating limits".

213. In addition, the GDA technical guidance (Ref. 40) contains expectations regarding the development of operating rules during GDA. These are generally at the individual discipline level, but the fundamental expectation remains that an output from the safety case should be the identification of operating rules that must be implemented to ensure that the plant is operated within a safe envelope. Collectively these set the expectation that, while operating rules will be developed fully by a licensee in a site-specific phase, there is still the need for the RP to demonstrate its approach to operating rules during GDA with a focus on those that are the most safety significant.

214. I therefore focussed my assessment of the RP's approach to operating rules on:

- The RP's approach to developing operating rules and the GDA scope for those
- Identification of operating rules within the generic UK HPR1000 safety case, including the sampling of the methodology for developing Operational Technical Specifications (OTS) and its implementation.
- Suitability of the operating rules' arrangements for transfer to a licensee in a manner that facilitates its understanding and further development.

215. The key SAPs (Ref. 2) applied within my assessment were SAPs SC.4 and SC.6, and NS-TAST-GD-035, 'Limits and Conditions for Nuclear Safety (Operating Rules)' (Ref. 25). The GDA technical guidance (Ref. 40) also contains relevant expectations for operating rules. I have also considered the relevant aspects of IAEA Safety Guide NS-G-2.2 'Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants' (Ref. 34), although the ONR TAG (Ref. 25) has already considered this guidance.

4.6.1.1 General Approach to Operating Rules during GDA

216. PCSR Chapter 31 (Ref. 7) summarises the approach adopted by the RP to the development of operating rules during GDA. The RP's approach is based mainly upon IAEA guidance (Ref. 34) in particular, with some use of United States Nuclear Regulatory Commission's (US NRC) methodologies (particularly for Technical Specifications (TS)). The RP stated that the same approach is used for its domestic plants.

217. The RP's submission, 'Generic Limits and Conditions for Normal Operation' (Ref. 18), and to a lesser extent PCSR Chapter 31, explains the scope of operating rules development during GDA. It should be noted that I found lack of clarity and justification over the scope, along with an absence of links between the operating rules identified in the previous revision of the 'Generic Limits and Conditions for Normal Operation' (Ref. 18) and the wider safety case for UK HPR1000. I raised RQ-UKHPR1000-1681 (Ref. 12) to clarify these matters and the RP improved the linkages to the safety case and provided further information, including Figure 3 (Ref. 7) below that summarises the GDA scope.

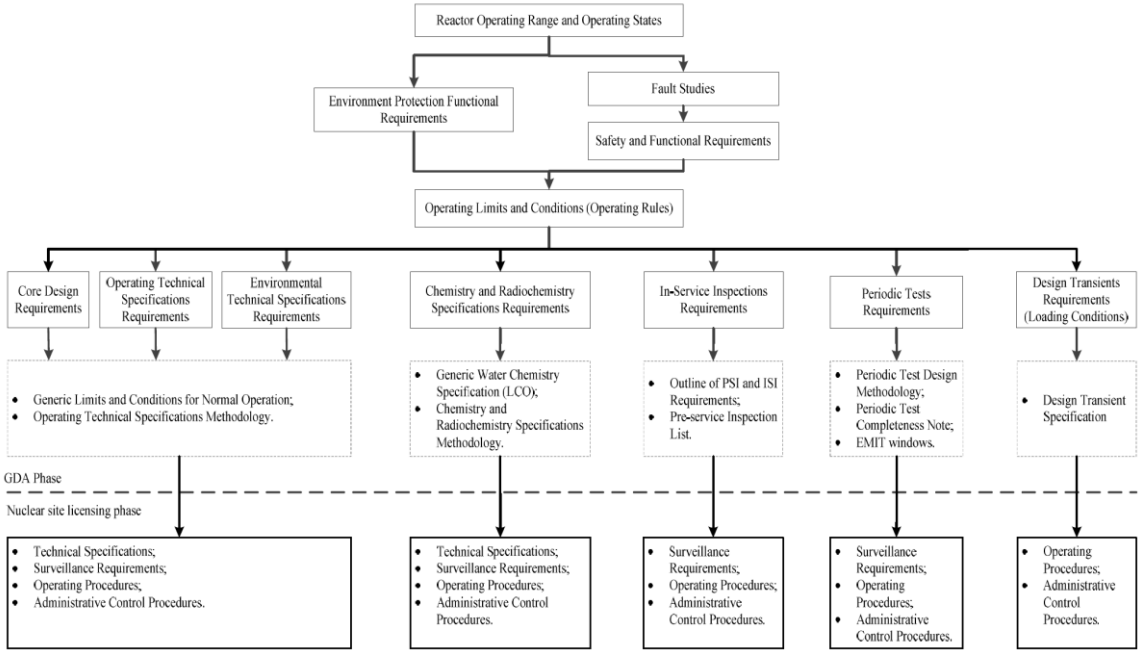

Figure 3: Scope of operating rules development during GDA

218. As seen in Figure 3, the RP considers there to be seven categories of operating rules: OTS, Environmental Technical Specifications (ETS), Chemical and Radiochemical Specifications (CRS), ISI, Periodic Testing (PT), loading condition (design transient) requirements and core design requirements. It should be noted that OTS, ETS and CRS are considered as TS. Figure 3 includes the main types of operating rules I would have expected to see and covers the breadth of operating rules that will need to be developed. I am satisfied that this approach is adequate for GDA.

219. The RP has also provided methodologies associated with TS, PT, ISI, Preventative Maintenance (PM) and procedures which detail how a licensee could use the generic safety case information to develop TS, surveillance programmes and operating procedures. I sampled these submissions later in my assessment.

220. These seven categories are intended to be supported by operating documentation that a licensee will develop. Based upon its own experience of operating nuclear plants in China, the RP suggested a likely approach that could be adopted (noting that this is a licensee's decision), citing four document categories: namely TS, surveillance requirements, operating procedures and administrative procedures. I have not assessed this given it is subject to change by a licensee, but it does demonstrate an important aspect of the RP's approach which is that the identified operating rules are graded such that the most important operating rules have the greatest prominence, for example as part of TS. This is consistent with international and ONR's guidance and is similar to approaches I have seen adopted by operating facilities in the UK.

221. The RP's submission (Ref. 18) confirms that the RP considers operating rules to apply during all operating states from power operation to shutdown, including maintenance conditions and it specifies which states apply to each of the defined operating rules This is consistent with ONR's expectations in NS-TAST-GD-035 (Ref. 25).

222. Similarly, in the 'Generic Limits and Conditions for Normal Operation' report (Ref. 18), the RP explains the relationship between operating rules and the different levels of defence in depth. I have not assessed the detailed allocation of operating rules to the different levels, but I consider it positive that the RP has considered its approach in these terms. It is clear that, at this stage of GDA, most of the identified operating rules

currently reside at level 3 given they originate largely from safety analysis but the intention to expand this is clearly stated. I am encouraged by this approach, which is consistent with my expectations.

223. The RP also acknowledges that the most significant operating rules in respect of nuclear safety are identified from criteria that include initial condition of plant normal operation, safety measures to be carried out in design basis faults, PSA or engineering experience amongst other factors. I am content that, in principle, this is a suitably broad approach to ensure that operating rules are identified and underpinned by the safety case. The RP does note (Ref. 18) that further parts of the safety case will need to be considered post-GDA, for example DEC, internal and external hazards analysis, in defining the complete operating rules. I consider this further in sub-section 4.6.1.2.

224. Based on the outcome of my assessment of the approach to operating rules proposed by the RP, overall, I am content that the general approach and scope during GDA is adequate. The RP has identified several important aspects of its approach which are consistent with relevant guidance and has provided clarity over where further development by a licensee will be needed.

4.6.1.2 Identification of Significant Operating Rules during GDA

225. For GDA two main reports, the 'Generic Limits and Conditions for Normal Operation' (Ref. 18) and 'Generic Water Chemistry Specification' (Ref. 79), with their supporting references, set out what the RP considers to be the most safety significant operating rules identified from the generic safety case during GDA. These operating rules are:

- OTS and limits and conditions for normal operations which can be found in the 'Generic Limits and Conditions for Normal Operation' report (Ref. 18)
- CRS which can be found in the 'Generic Water Chemistry Specification' report (Ref. 79)

226. In this section, I have sampled the methodology for identifying OTS (Ref. 80) and its implementation and assessed that the operating rules within the RP's submissions (Ref. 18) and (Ref. 79) are linked and underpinned by relevant safety case documents.

Operating Technical Specifications Methodology (Ref. 80)

227. The approach to defining an operating rule such as an OTS is to apply the first two steps identified in the RP's OTS methodology report (Ref. 80) which involve defining functional availability requirements and their associated operating modes.

228. In the first step, the RP identifies the applicable 'safety features' and identifies their availability requirements using the engineering documents (such as the SDMs). The RP cites the 'UK HPR1000 Fault Schedule' (Ref. 81) as an important input. I note that the term safety feature is inconsistent with other aspects of the generic UK HPR1000 safety case, which use 'safety functions'. This is an artifact of the development of this document from reference plant information in the first instance. There are other examples of such inconsistencies in terminology and nomenclature, but these do not undermine the outcomes of the report. I therefore consider this to be a minor shortfall.

229. In the second step, the RP determines the TS requirements – namely the initial conditions used within the fault analysis and operability requirements consistent with the analysis rules. To further describe its approach, a worked example based on the RIS [SIS] is provided in the 'Generic Limits and Conditions for Normal Operation' report (Ref. 18). This example clarifies how the fault schedule (Ref. 81), RIS [SIS] SDM (Ref. 82) and relevant design basis analysis are used to inform the defined OTS requirement. This clearly explains the underpinning by the generic safety case

documents, and it is clear why the resulting OTS requirement is consistent with the underpinning safety analysis.

230. I requested the 'System OTS of Safety Injection System (RIS) [SIS]' report (Ref. 19) which is a translation of the reference design report that defines the OTS for the RIS [SIS] to check the consistency between the OTS defined by the RP's proposed process with the OTS from the reference plant. I am content that both documents provide similar information.

OTS Requirements (Ref. 18)

231. The OTS requirements identified in the 'Generic Limits and Conditions for Normal Operation' report (Ref. 18) cover two aspects:

- Safety limits – Operating limits which can influence the release of radioactive material from the fuel, for example temperatures of fuel. This method is in accordance with NS-G-2.2 (Ref. 34).
- Safety system settings – Settings for variables in automatic protection devices which have significant safety functions. These include those which cause the reactor to trip to suppress a transient, result in other automatic actions to prevent safety limits from being exceeded or initiate operation of engineered safety systems.

232. The RP's submission (Ref. 18) identifies safety limits that must not be exceeded for parameters relating to primary pressure, thermal power, coolant temperature and core parameters amongst others. These are derived from a number of generic safety case design documents. Tables are also provided which detail the settings for automatic reactor trips, and actuation settings for safety systems and support systems. Again, these are clearly linked to relevant engineering documentation. The tables contain information on applicable operating modes, channels and setpoints (where available). I also note that the tables make use of the RP's requirements management coding developed in response to RO-UKHPR1000-0004 (discussed in sub-section 4.5.1). This further enhances the traceability of these requirements.

233. The details within these tables have been assessed by individual disciplines, as appropriate, however based on my own general knowledge of the generic UK HPR1000 safety case I am content that this represents a suitable approach for GDA, with further development by a licensee. The tables do identify many of the most important operating rules based on the current development of the generic safety case for UK HPR1000.

Limits and Conditions for Normal Operation (Ref. 18)

234. The RP uses the criteria of the US NRC's 10CFR50.36 (Technical Specifications) (Ref. 83) to define its limits and conditions for normal operation. These are standard criteria used in the US and allow the RP to identify which SSCs need to be considered for inclusion into TS. The resulting list of SSCs is given in the RP's submission (Ref. 18), and includes all the safety systems, many of the supporting systems and some radioactive waste management systems.

235. As noted previously, this does exclude some aspects of the safety case which are likely to contain or input into such high hazard operating rules (such as DEC and hazards analysis). The RP does state that it expects that this list will expand when other parts of the safety case are considered by a licensee. For the purposes of my own assessment this is a reasonable approach, but this may not apply to individual discipline assessments which will be considering specific operating rules in more detail. I also consider that these omissions for GDA will be significant unless

satisfactorily resolved by a licensee. I therefore consider this to be an Assessment Finding.

AF-UKHPR1000-0111 – The licensee shall, as part of implementing site specific operating rules, ensure that the approach includes all important aspects of operation and management, in view of the type and magnitude of hazards involved. This should include those aspects not fully developed during GDA including identified hazards, all levels of defence in depth and human related claims.

236. The RP's submission (Ref. 18) presents the operating rules applicable to the SSCs in five tables covering environmental requirements, fuel and core design, mechanical engineering, instrumentation and control, and electrical engineering. For each, parameters, systems, applicable operating modes, OTS / ETS requirements, safety function requirement coding, corresponding criterion and links to underpinning safety case documentation are identified.

237. I have not assessed the detail in these tables as this is for technical disciplines to consider. However, I am content that the coverage and scope appears reasonable for GDA in demonstrating that a range of the most important operating rules has been identified.

Chemical and Radiochemical Specifications (Ref. 79)

238. PSCR Chapter 31 (Ref. 7) states that some CRS parameters will be part of the OTS, but many aspects (such as sampling frequency or expected values) will be detailed in the CRS. 'Generic Limits and Conditions for Normal Operation' (Ref. 18) does not discuss the approach adopted to develop the CRS from the 'Chemical and Radiochemical Specifications' report (Ref. 79), although it notes that this is another main input into the OTS. Similarly, the RP's submission (Ref. 79) itself only notes that "it is intended that this report could be used to define the plant chemistry and radiochemistry specifications in site-specific stage". I am content that a licensee would be able to develop the information in the 'Chemical and Radiochemical Specifications' (Ref. 79) into the CRS and OTS as appropriate, and this submission (Ref. 79) does contain a significant resource to do so. Therefore, despite the lack of clarity provided during GDA on how this may be achieved, I am content this represents a minor shortfall.

4.6.1.3 Further Development of Operating Rules Post-GDA

239. As shown in Figure 3, there are some aspects of operating rules that the RP has not developed during GDA. Instead, it has provided methodologies for how a licensee could use the generic safety case information to develop TS, surveillance programmes and operating and administrative procedures. Those aspects not considered earlier in my assessment include:

- In-service inspection – The RP defines ISI as a preventive maintenance process involving the use of non-destructive testing for nuclear pressure mechanical components at scheduled intervals during operation. The RP has outlined the ISI requirements and those have been considered in the ONR Structural Integrity assessment (Ref. 84).
- Periodic testing – PT aims to verify that the defined safety functions can be delivered during the plant lifetime, based upon testing against defined criteria, under required configurations, according to a predetermined frequency and method. The RP has provided the PT methodology and detailed aspects, such as the PTCN document (Ref. 75). PT has been considered by several disciplines during GDA and is reported in their individual assessment reports, as appropriate.

- Loading conditions – The integrity of SSCs is verified against design loading conditions which are derived from the operating conditions that might occur (during normal operations and faults). The loading conditions will affect the surveillance requirements. This is described in PCSR Chapter 17 (Ref. 85) and considered in the Structural Integrity assessment (Ref. 84).
- Maintenance – The RP's approach to EMIT for UK HPR1000 was the purpose of RO-UKHPR1000-0021 (Ref. 22) which is outside the scope of my assessment. However, I have assessed PCSR Chapter 31 (Ref. 7) that details the RP's approach to maintenance and 'Generic Limits and Conditions for Normal Operation' (Ref. 18). Both documents use the outputs from RO-UKHPR1000-0021 in deriving the operating rules, particularly regarding the available window under which maintenance can be performed.
- Ageing and degradation management – The RP has provided high level guidance (Ref. 86) on the expected approach to develop an ageing and degradation management programme. This submission (Ref. 86) identifies appropriate operating rules and has been assessed by different ONR disciplines.

240. Based upon my assessment, I am content that the RP has defined how the generic safety case will need to be further developed by a licensee to consider other operating rules. Some aspects have already been subject to some development, and others have been assessed outside my own assessment, but I am clear that overall sufficient has been provided for GDA. I am satisfied that the intent of ONR's guidance (Ref. 1, Ref. 25, Ref. 40) has been met in this regard. This does not preclude other specific shortfalls being identified at the discipline level.

4.6.1.4 PCSR Assessment – Chapter 31 – Operational Management

241. The RP updated version 1 of the PCSR to reflect the work undertaken during Step 4 of GDA and provided ONR with an advance copy of the PCSR version 2 (Ref. 7). I reviewed this report and have later checked the final version of the PCSR to ensure that the outcome of my assessment remained the same (Ref. 87).

242. As explained previously, PCSR Chapter 31 summarises the approach adopted by the RP to the development of operational rules during GDA and provides links to the relevant methodologies and guidance. This chapter has been updated to include further information on the scope of operating rules during GDA, the RP's approach to EMIT as a result of the work carried out under RO-UKHPR1000-0021, and links to the methodologies developed during Step 4 of the GDA and described in my assessment (see previous sub-sections).

243. I am content that this update is appropriate for a high-level document such as the PCSR and that it provides the overview to operating rules referring to key documents such as the 'Generic Limits and Conditions for Normal Operation' (Ref. 18) and Chemical and Radiochemical Specifications (Ref. 79).

4.6.2 Strengths

244. Following my assessment of the RP's approach to operating rules for the UK HPR1000, I have identified the following strengths:

- The RP has defined its approach for defining operating rules, which is consistent with relevant guidance and is based upon its previous experience for operating plants.
- A range of the most safety significant operating rules has been defined explicitly for UK HPR1000.

- The RP has improved the linkages to the generic UK HPR1000 safety case and better defined the further development of operating rules necessary by a licensee.
- The RP has provided methodologies and guidance that a licensee would be able to further develop and implement in the site-specific phases.

4.6.3 Outcomes

245. Following my assessment of the RP's approach to operating rules for the UK HPR1000, I have identified that whilst the arrangements are adequate for GDA, there is a shortfall that must be resolved after GDA by the licensee. Therefore, I raised one Assessment Finding regarding the further development of the approach to operating rules to include important aspects of operation and management, such as all levels of defence in depth and human related claims.

246. I have identified two minor shortfalls in sub-section 4.6.1.2.

247. It should be noted that detailed assessment of specific operating rules is undertaken by the relevant ONR technical disciplines.

4.6.4 Conclusion

248. Based on the outcome of my assessment I consider that the RP's approach to operating rules is consistent with relevant guidance and its implementation is adequate. The RP has provided sufficient evidence of the implementation of the approach to derive some of the most safety significant operating rules, including the linkages to, and underpinning provided by, the safety case. The RP has developed methodologies and guidance for operating rules recognising that these will evolve as the detailed design progresses. I am content that sufficient has been provided for GDA and that a licensee would be able to further develop and implement this approach to operating rules in the site-specific phases.

249. I have concluded that the RP's approach to operating rules for the UK HPR1000 is adequate for the purposes of GDA. I have identified matters that need to be resolved by the licensee and captured these in an Assessment Finding.

250. Overall, I am satisfied that the operating rules approach developed by the RP meets the intent of ONR's SAPs, TAGs and the international guidance described in sub-section 4.6.1.

4.7 OPEX Arrangements

4.7.1 Assessment

251. ONR expected (Ref. 40) the RP to present clear evidence that OPEX has been used in the design of the UK HPR1000. This is applicable to all technical topics, however, some topics, such as Chemistry, Radiological Protection, Human Factors and Decommissioning, place a greater emphasis on using OPEX as a source of supporting evidence to make a robust demonstration of safety. I refer to those technical disciplines as 'OPEX-dependent' technical disciplines in this report.

252. The OPEX-dependent technical disciplines identified a number of gaps in the use of OPEX, like a lack of systematic approach to OPEX gathering, OPEX was often limited to CGN OPEX, and there was insufficient justification on the applicability of the OPEX to support the RP's conclusions. However, a more fundamental shortfall was that while OPEX was cited in the generic safety case and key safety arguments made, or conclusions drawn on the basis of that OPEX, the OPEX itself, in other words the data,

was often not presented in the documentation. As a result of these shortfalls in OPEX, ONR raised RO-UKHPR10000-0044 (Ref. 10).

253. My assessment of the use of OPEX in the safety case has focused on the RP's arrangements for identifying, capturing, and justifying the applicability of relevant OPEX and on the demonstration of the application of those arrangements (Actions 1 and 2 in RO-UKHPR10000-0044). Assessing how OPEX is identified and used is cross-cutting and wide reaching, so I worked closely with the OPEX-dependent disciplines to sample the implementation of the OPEX methodology. The submissions that form part of my assessments are described in sub-sections 4.7.1.1 and 4.7.1.2.

254. It should be noted that the technical judgements on whether OPEX is suitable and sufficient are matters for ONR's specialists and those are reported, as appropriate, in relevant technical topic assessment reports (Ref. 3).

255. The key SAPs (Ref. 2) applied within my assessment of the RP's OPEX arrangements were SAPs MS.4 and SC.7 and the associated TAGs, NS-TAST-GD-005, 'Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable)' (Ref. 23), NS-TAST-GD-050 'Periodic Safety Reviews (PSR)' (Ref. 26), NS-TAST-GD-051, 'The Purpose, Scope and Content of Safety Cases' (Ref. 27). Although TAG NS-TAST-GD-050 is not directly relevant to a GDA, the principles still broadly apply to the production of a generic safety case, and therefore I have considered it during my assessment.

4.7.1.1 Arrangements for Identifying, Capturing, and Justifying the Applicability of Relevant OPEX

256. To demonstrate how OPEX is identified, captured, and used in the UK HPR1000 design and safety case, the RP submitted one of its existing procedures, 'Management Rules on Experience Feedback of UK HPR1000 GDA Project' (Ref. 20) and developed a brand-new methodology, 'Methodology for Use of OPEX in UK HPR1000' (Ref. 21). I assessed both documents and summarise my assessment below.

257. The existing procedure (Ref. 20) defines and explains key roles and responsibilities – including both individuals' and wider organisational functions. The procedure also describes the tools used by the RP to source and record OPEX, for example 'the experience feedback system'. Annex 2 of the existing OPEX procedure (Ref. 20) summarises sources of OPEX and provides OPEX 'channel' descriptions. The OPEX sources cited are wide ranging – including Chinese domestic sources and many other international sources. From a regulatory perspective, many of these sources are easily recognisable as organisations which ONR regards as being reliable and appropriate sources of good practice. The RP's existing procedure (Ref. 20) also contains templates used by the RP to standardise its approach to sourcing, collating and managing OPEX. I consider that the RP's management rules on OPEX (Ref. 20) provides a well-documented procedure, which appears to be mature and well-established within the RP's organisation.

258. The new methodology for managing OPEX (Ref. 21) presents further information on the RP's arrangements for managing OPEX, but with a greater emphasis on how OPEX is to be considered in the demonstration of ALARP and Best Available Techniques (BAT) and during optioneering. The report describes an eight step process the RP follows, starting from identification (step 1) and collection of OPEX (step 2), through to determining how OPEX may be used in making the safety case (step 5) and ending with how a robust justification should be prepared regarding the suitability and sufficiency of the OPEX (step 8). Overall, I consider the new methodology to be a welcome and necessary addition to the generic UK HPR1000 safety case.

259. Steps 5-8 of the RP's process described in the new methodology (Ref. 21) provide information on how RP personnel justify OPEX, and how that information should be presented in the generic UK HPR1000 safety case. In step 5, the RP establishes the importance of first determining how OPEX is intended to be used in the generic UK HPR1000 design and safety case. In my opinion, this ensures a greater focus on what OPEX to source, and, more importantly, it moves the focus onto why the OPEX is being sourced. In my view, this was an important step in the overall 'journey' of justifying the applicability of OPEX. Step 6 of the RP's process is a screening exercise. Step 7 then provides guidance on use of OPEX, identifying three specific uses, 'input use', 'justification use' and 'optioneering use'. Overall, based on the information presented in the new methodology, I am satisfied that the RP has developed suitable arrangements to identify applicable OPEX.

260. The final step in the process, step 8, provides guidance on justification, largely in the form of a list of prompts to consider. The main aim of the step is to justify that all relevant sources of OPEX have been appropriately considered in the generic UK HPR1000 design and safety case. On the basis of this information, I judge that the RP has provided an adequate process prescribing how the applicability of OPEX should be justified and presented in the generic UK HPR1000 safety case.

261. The new methodology also addresses the RP's approach to identifying and managing OPEX which is applicable to multiple topics and explains its approach to non-nuclear sector OPEX listing several sources of non-nuclear sector OPEX. Overall, I am satisfied with the evidence provided to manage interfaces between technical topics and with the RP's approach to considering a wider range of non-nuclear experience. This last point is consistent with the expectations of SAP SC.7.

262. One of the areas of concern was that the RP's approach was leading to a very narrow OPEX selection. Therefore, during my assessment, I sampled this area in greater depth because I was also aware of several examples where the RP had claimed that it was unable to access certain pieces of OPEX (data), owing to constraints around Intellectual Property Rights (IPR) and 'commercial factors'. I raised an RQ asking the RP to provide additional information on its approach to managing constraints. The RP explained that when a particular constraint is identified, a 'project feedback management committee' is established, which comprises senior members of the RP's organisation. The committee is tasked with finding solutions to overcome the identified constraint(s). The RP provided examples on how it has overcome IPR issues, and some of those examples included performing trials. I consider that adequate evidence has been presented to demonstrate that the RP did not limit the selection of OPEX and could overcome constraints related to OPEX.

4.7.1.2 Demonstration of the Application of the RP's OPEX Arrangements

263. In the demonstration of the application of the OPEX arrangements the RP:

- Identified the OPEX-dependent topics.
- Applied the new methodology to identify any shortfalls in the OPEX-dependent topics.
- Provided evidence (12 submissions) to demonstrate the practical application of the new OPEX arrangements. Further details of those submissions can be found in ONR's closure note for RO-UKHPR1000-0044 (Ref. 88)

264. I reviewed the 'Sample Submission Programme for OPEX-Dependent Topics' (Ref. 89) where the RP developed the criteria and guidance to identify the technical disciplines with greatest reliance on the use of OPEX (OPEX-dependent topics). The RP concluded that these areas are chemistry, radiological protection, source term, radioactive waste management, decommissioning, and spent fuel management,

human factors and environmental. After reviewing the RP's submission (Ref. 89) I am of the opinion that the RP has developed and implemented a robust process to define OPEX-dependent topics. From a regulatory perspective, its decision-making criteria capture the key aspects I expect to be considered. For example, prompts on safety function categorisation, classification of SSCs, links to risks and hazards and their magnitude, and the role of OPEX in justifying that relevant risks are reduced to ALARP. Furthermore, based on first principles and my knowledge of safety cases as a regulator, the OPEX-dependent topics identified by the RP are consistent with ONR's expectations.

265. The 'Sample Submission Programme for OPEX-Dependent Topics' (Ref. 89) also presents the outcome of the gap analysis, where the new methodology was applied to existing OPEX reports (OPEX summary reports and OPEX application reports). The gap analysis concluded that 17 of these reports needed modifying in that either a brand-new document was required, or updates to existing reports were needed. It was agreed that from the 17 reports, 12 reports would be sampled by ONR, and the RP developed a well-defined plan to address the gaps identified in this submission (Ref. 89).

266. The final part of my assessment was to consider the adequacy of the 12 RP's submissions. To do this I engaged ONR specialist inspectors in Nuclear Liabilities Regulation, Radiological Protection, Chemistry and Human Factors. Normal operational source term(s) was also considered.

267. The key themes arising from the assessment of the 12 submissions were:

- Some specific gaps with integrating OPEX into the generic safety case were still apparent. The gaps were associated with technical judgements on the suitability of the OPEX as safety case evidence and those were considered by the technical disciplines in their assessment reports. As stated before, the technical suitability of the OPEX is outside of the scope of my assessment.
- There were some issues with traceability to the sources of OPEX in some documents.
- Some quality issues with some documents were noted. However, the specialists' view was that, overall, these were not significant.
- Taken as standalone documents, in some cases, the submissions were not sufficient to be able to draw definitive conclusions about the breadth and depth of the RP's integration of OPEX into the generic safety case. Some specialists had to rely on their knowledge of the wider safety case. However, when taken together, in the context of the new OPEX methodology, overall, they concluded that they were satisfied with the RP's approach.

268. Despite some of the matters identified, the consensus view from all specialists was that overall the RP had adequately demonstrated the application of the new OPEX methodology. Further details of my assessment can be found in the closure note for RO-UKHPR1000-0044 (Ref. 88).

269. I followed the OPEX implementation with a workshop with the RP (Ref. 53) to also gain visibility of the OPEX arrangements in the 'non-OPEX dependent' technical areas. The RP explained that the OPEX arrangements were applied to non-OPEX dependent technical areas and the outcome was summarised in the OPEX reports for each technical discipline. Two examples of how OPEX was sourced and employed were presented (steam generator decommissioning and a structural integrity example of OPEX). The arrangements as described, supported by sampling of relevant documents, confirmed that the same approach to OPEX was used in both 'OPEX dependent' and 'non-OPEX dependent' technical areas.

270. As already indicated above, the assessment of the technical adequacy of the OPEX used in the generic UK HPR1000 design has been carried out at the technical topic level and therefore reported as appropriate in the relevant technical topic assessment reports.

4.7.1.3 PCSR Assessment – Chapter 20 – OPEX Arrangements

271. The RP updated version 1 of the PCSR to reflect the work undertaken during Step 4 of GDA and provided ONR with an advance copy of the PCSR version 2 (Ref. 6). I reviewed this report and have later checked the final version of the PCSR (Ref. 60) to ensure that the outcome of my assessment remained the same.

272. The RP updated Chapter 20 of the PCSR to reflect the new OPEX arrangements. I have assessed the update (Ref. 6). The RP has included a new section that describes the importance of the use of OPEX, references the existing procedure (Ref. 20) and the new OPEX methodology (Ref. 21) and explains how OPEX is used in the ALARP demonstration for the UK HPR1000. This new section also mentions the topic specific OPEX analysis reports.

273. While the update does not specifically mention the gaps addressed by the new OPEX methodology, it states that the new methodology is used by the various technical topics to gather OPEX from a wide range of sources. I am content that this update is appropriate for a high-level document such as the PCSR and that it is consistent with the information in the RP's OPEX methodology.

274. I have checked the OPEX section in the final version of the PCSR (Ref. 60), and I can confirm that the outcome of my assessment remains the same.

4.7.2 Strengths

275. Following my assessment of the identification and use of OPEX in the UK HPR1000, I have identified the following strengths:

- The RP has developed a new OPEX methodology that has improved how different sources of OPEX have been identified, captured and analysed.
- The new OPEX methodology has clarified how dependencies and interfaces between different topics have been managed and how OPEX from non-nuclear sectors has been considered.
- The RP has provided evidence to demonstrate how several constraints around access to OPEX have been managed and overcome during GDA.
- The RP has provided sufficient evidence to demonstrate that a robust process was applied to identify OPEX-dependent topics and has addressed the gaps from the OPEX gap analysis.
- The RP has developed OPEX summary reports for all disciplines, which have been used as key inputs into the ALARP demonstration reports for each topic. These reports have improved the overall visibility of how relevant OPEX is identified, screened, and justified as being applicable.
- PCSR Chapter 20 provides an adequate summary of the OPEX arrangements with references to the key supporting information.

4.7.3 Outcomes

276. Following my assessment of the identification and use of OPEX in the UK HPR1000, I have not identified Assessment Findings. However, the technical judgements on the suitability of the OPEX as safety case evidence to support the relevant claims and argument are reported, where appropriate, in the Step 4 topic assessment reports (Ref. 3).

4.7.4 Conclusion

277. Based on the outcome of my assessment of the identification and use of OPEX in the UK HPR1000, I have concluded that the RP has established adequate arrangements for identifying, capturing and analysing OPEX. The RP has also demonstrated the implementation of those arrangements. I am satisfied that relevant expectations derived from SAPs MS.4 and SC.7 and TAGs, NS-TAST-GD-051, NS-TAST-GD-005, and relevant parts of NS-TAST-GD-050 are met.

4.8 Demonstration that Relevant Risks Have Been Reduced to ALARP

4.8.1 Assessment

278. A nuclear licensee or dutyholder in the UK has a legal requirement to reduce risks SFAIRP. NS-TAST-GD-005, 'ONR Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable)' (Ref. 23) provides technical guidance to ONR inspectors on what they should expect of a dutyholder in meeting this. The term ALARP is usually used when referring to the level to which risks must be reduced in order to meet the legal requirement and is considered equivalent to SFAIRP. Also, ONR's expectation is that the safety case should demonstrate how risks are reduced to ALARP. This expectation is set out in SAP SC.4 (Ref. 2).

279. Annex 2 to NS-TAST-GD-005 gives specific advice on ALARP for new reactors. It indicates that nominally at the design stage, the proposed designs (for GDA) are essentially complete in terms of the overall concept and major systems and have reached that stage after many years of development and optimisation in non-UK regulatory environments. This is indeed the case for the UK HPR1000 design, in which the design is an evolution of the CPR1000 design in the Chinese nuclear fleet.

280. In terms of reducing the risks to ALARP, the majority of the cross-cutting topics reported here are improvements to existing processes and ultimately improvements to the safety case. Therefore, in this section I judge how those arrangements have contributed to the demonstration of the reduction of the risks to ALARP. I have included a final sub-section to summarise my judgement against the demonstration that relevant risks have been reduced to ALARP.

4.8.1.1 Nuclear Safety Principles

281. The RP has developed its own nuclear safety principles in the PCSR Chapter 4 (Ref. 90). Those principles are based on international good practice and are aligned with ONR's SAPs.

282. The first RP's general safety and design principle is 'Reducing the risks to ALARP' and the applicability of this principle to the UK HPR1000 design is the key contributor to the ALARP demonstration. The rest of the principles have been described in sub-section 4.2, and in summary, all the RP's NSPs, if applied to the design, will contribute to the risk reduction. For example, the radiation safety requirements and the use of applicable codes and standards are two NSPs directly linked to the expectations in NS-TAST-GD-005 regarding the demonstration of ALARP.

283. The application of the RP's NSPs to the design has been considered at a topic level and reported, where appropriate, in the topic reports (Ref. 3). Therefore, whilst I cannot judge the specific application of the NSPs, I consider that the NSPs have provided a good basis for the RP to demonstrate that the risks are reduced to ALARP.

4.8.1.2 Safety Case Development

284. ONR's expectation is that the safety case should demonstrate how risks are reduced to ALARP (SAP SC.4). In order to provide this demonstration, the RP needs to develop and deliver a good quality comprehensive safety case, which was the aim of the safety case development cross-cutting work.

285. The improvements made under this cross-cutting theme (see sub-section 4.3) were key to demonstrating that the relevant risks were reduced to ALARP. For example, the safety case development strategy report (Ref. 13) and the production strategy reports for each technical discipline provided the golden thread to the evidence that underpins the RP's ALARP claims and arguments. Also, the safety case health check was one of the main drivers for the improvements and enhancements made in the RP's topic specific ALARP demonstration reports and in the 'Holistic ALARP Demonstration Report' (Ref. 55).

286. The technical assessment of ALARP demonstration has been carried out at a topic level and in the Step 4 summary report (Ref. 4), but I consider the safety case development as one of the main vehicles for providing that demonstration.

4.8.1.3 Commitments Management

287. As per the previous cross-cutting topics, the RP's arrangements for managing commitments and their appropriate implementation in the safety case have contributed to the ALARP demonstration. Many of the commitments were raised to address gaps or to carry out further work that ultimately contributed to the claim that the risks are reduced to ALARP. Also, the RP identified and captured areas (post-GDA commitments) for further development after GDA, which will be addressed by the licensee during the detailed design phase.

288. Whilst the technical contribution of commitments to the ALARP demonstration has been considered, where appropriate, at a topic level, I consider that the process for capturing and incorporating those in the safety case has contributed to underpinning the reduction of risk to ALARP.

4.8.1.4 Safety Case Requirements Management

289. The ability to identify and trace implementable requirements through the safety case is key to the golden thread and to develop a good quality and comprehensive safety case. In order to develop the requirements management arrangements, the RP carried out appropriate optioneering and provided an adequate justification of the selected option. This is aligned with the expectations in TAG, NS-TAST-GD-005 (Ref. 23).

290. As per the previous cross-cutting topics, I consider that the RP's arrangements for managing implementable safety case requirements have contributed to the ALARP demonstration, in terms of providing a process to identifying and tracing the golden thread supporting the safety case.

4.8.1.5 Approach to Operating Rules

291. The demonstration that the plant can be operated within a safe envelope via implementation of operating rules is key to the demonstration of the reduction of the risk to ALARP. Operating rules are a fundamental output of any safety case and provide the limits and conditions necessary for nuclear safety.

292. My assessment of the RP's approach to operating rules, including the methodologies for identifying them, confirmed that those were consistent with RGP and based on

OPEX. Therefore, I consider that the RP's approach provides the high-level arrangements and supports the demonstration of ALARP.

4.8.1.6 OPEX Arrangements

293. The RP's ALARP methodology (Ref. 55) includes the gathering of OPEX and the systematic review of the design against RGP and OPEX to identify further improvements. Therefore, the improvements made under this cross-cutting topic had a direct impact on the reduction of the risks to ALARP.

294. In summary, based on the new OPEX arrangements, each discipline has collected OPEX, and reviewed the design against it to identify potential improvements. The OPEX is reported in the OPEX reports for each discipline and the review of OPEX and potential improvements are reported in the ALARP demonstration reports for each discipline.

295. The technical assessment of OPEX reports and the ALARP demonstration reports have been carried out at a topic level. However, I consider that the improvements made in the RP's OPEX arrangements directly contributed to the reduction of risk to ALARP, as the use of OPEX is part of the RP's ALARP methodology.

4.8.1.7 Summary

296. All six cross-cutting topics covered in this report are direct contributors to the demonstration that risks have been reduced to ALARP in terms of:

- providing safety and design principles;
- improving to the golden thread in the safety case; and
- improving the RP's ALARP methodology.

297. During the development of the NSPs and the new arrangements / methodologies, the RP has considered international RGP and UK practice. Also, the RP has carried out adequate optioneering in the development of the requirements management arrangements and the new OPEX methodology.

298. Overall, I consider that the six cross-cutting topics covered here are aligned with ONR's guidance in TAG, NS-TAST-GD-005 (Ref. 23) and SAP SC.4, in terms of how they have been developed and their contribution to reducing the risks to ALARP.

4.8.2 Strengths

299. The majority of the cross-cutting topics covered in this report relate to improvements to processes, which themselves contribute to the ALARP demonstration. Therefore, in terms of demonstrating that the relevant risks have been reduced to ALARP, my assessment has identified the following strengths:

- The RP has developed adequate NSPs that if applied correctly will contribute to the ALARP demonstration.
- The improvements made on the safety case development, commitments management, and requirements management have contributed to developing an adequate safety case by improving the golden thread.
- The new OPEX methodology has improved the RP's ALARP methodology implementation.
- The RP has developed its approach to defining operating rules, improving the linkages to the safety case.

4.8.3 Outcomes

300. My assessment of the RP's demonstration that relevant risks have been reduced to ALARP in relation to the six cross-cutting topics covered in this report did not identify any shortfalls additional to those identified elsewhere in this assessment report.

4.8.4 Conclusion

301. Based on my assessment, I conclude that the improvements made by the RP to the processes reported in this cross-cutting report have contributed to improving the safety case, which ultimately demonstrates the reduction of the risks to ALARP.

302. As a result, for the six cross-cutting topics, I am content that the RP has sufficiently addressed the expectations of SAP SC.4 and NS-TAST-GD-005 for GDA.

4.9 Consolidated Safety Case

4.9.1 Assessment

303. ONR expects (Ref. 1) that the consolidated Design Reference, PCSR, GSR and supporting documentation (tier 2 and 3 documents) incorporate, as appropriate, responses to RQs and, ROs, GDA commitments, FAPs, design modifications and safety case modifications.

304. My assessment of the safety case consolidation included:

- Chapters 4, 20 and 31 (Ref. 90, Ref. 6, Ref. 7) of the advance copy of the PCSR version 2 and PCSR version 2 to confirm that the chapters have consolidated RQs, ROs, GDA commitments, FAPs and safety case modifications from the cross-cutting topics reported here.
- A sample of tier 2 and 3 documents associated with the six cross-cutting topics.
- Overview of the adequacy of the safety case for the six cross-cutting topics.

305. The key SAPs applied within my assessment were SAPs SC.4 and SC.7 (Ref. 2), and TAG NS-TAST-GD-051, 'The Purpose, Scope and Content of Safety Cases' (Ref. 27).

4.9.2 Consolidation of PCSR Chapters 4, 20 and 31

306. The RP updated version 1 of the PCSR to reflect the work undertaken during Step 4 of GDA and provided ONR with an advance copy of the PCSR version 2 (Ref. 90, Ref. 6, Ref. 7). I reviewed this report and have later checked the final version of the PCSR (Ref. 41, Ref. 60, Ref. 87) to ensure it has been adequately consolidated.

307. In terms of consolidation, the advance copy of Chapter 4 (Ref. 90) of the PCSR did not reference the latest 'UK HPR1000 Design Reference Report' (Ref. 91), but this was addressed in the final version of the PCSR.

308. During my assessment of the NSPs, I raised two RQs and whilst the information provided by the RP in response to the RQs has not been directly incorporated into Chapter 4 of the PCSR, some of it was included in the requirements management procedure (Ref. 17) (see sub-section 4.9.3). I am therefore content that the RP has consolidated the relevant information adequately into pertinent safety case documentation.

309. In terms of consolidation, Chapter 20 of the PCSR (Ref. 6):

- Referred to the latest safety case development documents (Ref. 13, Ref. 37). The advance copy of the PCSR version 2 also included a FAP regarding the

'Safety Case Consolidation Summary Report' (Ref. 59). This FAP has been completed in the final version of the PCSR (version 2) (Ref. 60).

- In terms of commitments, the advance copy of the PCSR version 2 referred back to a non-consolidated version of GNSL's commitment procedure (Ref. 39) and it did not include the post-GDA commitment list (Ref. 15). Both matters have been addressed in the final PCSR version 2 (Ref. 60).
- The requirements management and the OPEX arrangements sections referred back to the latest submissions.

310. Chapter 31 of the PCSR has incorporated the information provided in the response to RQ-UKHPR1000-1681 (Ref. 92) regarding the RP's justification of the GDA scope of operating rules. I am satisfied that the RP has consolidated the response to my RQ into the PCSR.

4.9.3 Safety Case Consolidation – Tier 2 and 3 Submissions

311. In terms of consolidation of ROs, each RO has their own resolution plan and the submissions arising from the resolution plan become part of the safety case (and therefore consolidated). This report only covers two ROs, RO-UKHPR1000-0004 and RO-UKHPR1000-0044 (Ref. 22), and the outcome of those are the new processes and methodologies discussed in sub-sections 4.3, 4.4, 4.5 and 4.7. Therefore, I am satisfied that the submissions in response to RO-UKHPR1000-0004 and RO-UKHPR1000-0044 have been adequately consolidated.

312. Regarding the consolidation of RQs, for each of the cross-cutting topics I have sampled the incorporation of RQs' responses into the safety case. My assessment of the RP's safety case consolidation of the six cross-cutting topics has highlighted:

- NSPs – The RP incorporated part of the information provided in the responses to RQ-UKHPR1000-1111 and RQ-UKHPR1000-1295 (Ref. 12) in its requirements management procedure (Ref. 17). According to the RP's process, the NSPs are considered general requirements and so the route map provided in the RQs highlighted a number of documents that contain general requirements. Those documents are mentioned in the RP's procedure (Ref. 17) as sources of general requirements for specific disciplines. I consider this to be an adequate consolidation of the information in the RQs.
- Safety case development – RQ-UKHPR1000-1358 and RQ-UKHPR1000-1490 (Ref. 12) requested information about the safety case consolidation. The information within these RQs was incorporated into the 'Safety Case Consolidation Strategy' (Ref. 56). I am satisfied with the consolidation of these RQs.
- Commitments management – I raised RQ-UKHPR1000-1661 (Ref. 12) regarding the lack of criteria for post-GDA commitments in the RP's procedure (Ref. 14). The response to this RQ provided the criteria for post-GDA commitments that was included in the RP's procedures (Ref. 14, Ref. 39). I am satisfied with the consolidation of RQ-UKHPR1000-1661.
- Safety case requirements management – A significant number of RQs were raised on this cross-cutting topic, but for this assessment, I have sampled RQ-UKHPR1000-1676 (Ref. 12) regarding the lack of traceability of temperature and pressure requirements in the SFP (sub-section 4.5 – example 10). The RQ provided the traceability to the temperature requirements in the SFP, and the information was incorporated into Appendix S of the 'Requirements Management Summary Report' (Ref. 16).
- Approach to operating rules – I raised one RQ and I can confirm that the RP's response to RQ-UKHPR1000-1681 (Ref. 92) has been incorporated in the 'Generic Limits and Conditions for Normal Operation' report (Ref. 18).

- OPEX management – the RP's response to RQ-UKHPR1000-1218 (Ref. 12) clarified some aspects of its OPEX methodology (Ref. 21), but was not consolidated into the safety case documentation. The RQ's response provided greater visibility and specific worked examples of how the RP applied its OPEX methodology during GDA. Therefore, I did not expect the response to my RQ to be consolidated into the RP's safety case. Furthermore, the consolidation of this cross-cutting matter was essentially achieved by the RP in responding to the RO itself and the integration of the associated submissions, such as the new OPEX methodology and the implementation reports, into the safety case documentation. On that basis, I consider the safety case consolidation activities under this cross-cutting topic to be acceptable for GDA.

313. Based on my sampling, I judge that the safety case consolidation for the six cross-cutting topics is adequate.

4.9.4 Overall Safety Case Adequacy

314. The adequacy of the safety case for all six cross-cutting topics has been considered in several sub-sections within this report, which I summarise here.

315. Sub-sections 4.2 to 4.7 provide the outcome of my assessment of the safety case for the six cross-cutting topics, and this includes the relevant PCSR Chapters and the supporting documentation (tier 2 and 3 submissions). In some cross-cutting topics, my assessment has identified residual matters which I have captured as Assessments Findings or minor shortfalls in accordance with ONR's guidance (Ref. 1)

316. I have considered how the six cross-cutting topics have contributed to reduce the risks to ALARP in sub-section 4.8.

317. Finally, I am content with the safety case consolidation that the RP has undertaken for these six cross-cutting topics.

318. Based on the outcome of my assessment described in the previous sub-sections, I consider that the safety case for these six cross-cutting topics is sufficiently complete, consolidated, and adequate for GDA.

4.9.5 Strengths

319. Following my assessment of the generic UK HPR1000 safety case consolidation for the six cross-cutting topics, I have identified the following strengths:

- Chapters 4, 20 and 31 provide an adequate overview of the consolidated safety case with references to the key supporting information.
- The RP has adequately consolidated the tier 2 and 3 documents that I have sampled for the six cross-cutting topics.

4.9.6 Outcomes

320. My assessment of the consolidated safety case did not identify any shortfalls.

4.9.7 Conclusion

321. Based on the outcomes of my assessment I consider that the safety case as set out in PCSR Chapters 4, 20 and 31 version 2, together with the supporting documentation, accurately reflects the work done by the RP during Step 4 of GDA for the six cross-cutting topics. I am content that the RP has adequately met the expectations of SAPs SC.4 and SC.7 and TAG NS-TAST-GD-051, 'The Purpose, Scope and Content of Safety Cases'.

4.10 Comparison with Standards, Guidance and Relevant Good Practice

322. In Section 2, I have identified the most relevant standards, guidance and RGP. Throughout this assessment report I have described how I applied these in my assessment. This section provides a summary of the most relevant RGP, and a high-level statement as to how the design of the UK HPR1000 and the safety case has met these expectations.

323. The most relevant SAPs for my assessment are:

- NSPs: All SAPs – I have carried out a comparison between the RP's NSPs and ONR's SAPs, hence I have considered all SAPs with the exception of the siting SAPs. The RP's NSPs are aligned with the fundamental principles, key principles and the numerical targets.
- Safety case development: SAPs SC.1, SC.2, SC4, SC.7 and SC.8 – The RP has developed a safety case that aligns with the expectations of the safety case production processes, safety case process outputs that facilitate the safe operation, safety case maintenance and ownership.
- Commitments management: SAPs SC.1, SC.2 and SC.8 – The RP has developed an adequate commitment management process aligning with the expectations of the safety case production processes, safety case process outputs that facilitate the safe operation and safety case ownership.
- Requirements and assumptions management: SAPs SC.2, SC.4, SC.6, ECS.3, ECE.12, ECV.2, ECV.3 and EMT.1 – the RP has developed a process to identify requirements and trace them which ultimately will facilitate safe operation.
- Approach to operating rules: SAPs SC.4 and SC.6 – The RP has implemented its approach to deriving some of the most significant safety operating rules and underpinned those by the safety case. This aligns with the expectation that the safety case should identify all the limits and conditions necessary in the interests of safety (SAP SC.4) and justify the means of implementation for the operating limits and conditions (operating rules) (SAP SC.6)
- OPEX arrangements: SAPs MS.4 and SC.7 – The RP has established adequate arrangements for identifying, capturing and analysing OPEX. This aligns with ONR's expectation of learning from internal and external sources and maintaining the safety case.

324. The most relevant technical assessment guides applied in my assessment are:

- NS-TAST-GD-005, 'ONR Guidance on the Demonstration of ALARP' (Ref. 23) – For the purposes of GDA, the cross-cutting aspects assessed in this report will contribute to the reduction of the risks to ALARP by improving the golden thread in the safety case, establishing safety and design principles and improving the RP's ALARP methodology.
- NS-TAST-GD-009, 'Examination, Inspection, Maintenance and Testing of Items Important to Safety' (Ref. 24) – Although there are several Assessment Findings on requirements management, the RP's process is suitable to be used by the licensee to identify the EMIT requirements during the detailed design phase.
- NS-TAST-GD-035, 'Limits and Conditions for Nuclear Safety (Operating Rules)' (Ref. 25) – I applied the expectations within this guide proportionately to the level of development of this area in GDA and, overall, the RP's approach aligns with my expectations. For example, the RP considers operating rules to apply during all operating states, and this aligns with the expectation in the TAG.
- NS-TAST-GD-050 'Periodic Safety Reviews (PSR)' (Ref. 26) – Although PSRs are not directly relevant to GDA, the principles broadly apply to the production of a generic safety case. On that basis, the RP has provided sufficient evidence

to show that in relation to the OPEX arrangements, they have actively sought learning from external sources, including non-nuclear sectors.

- NS-TAST-GD-051, 'The Purpose, Scope and Content of Safety Cases' (Ref. 27) – For the purposes of GDA, the RP has developed an adequate safety case that provides a linkage between the top-level claims, sub-claims, supporting arguments and evidence for the cross-cutting topics covered by this report.

325. The RP has developed its NSPs based on international standards and guidance such as IAEA safety principles (Ref. 28) and safety standards (Ref. 29, Ref. 32, Ref. 33), and WENRA reference levels (Ref. 35, Ref. 36).

326. The RP has also demonstrated that the requirements management arrangements are aligned with IAEA safety standards (Ref. 30, Ref. 31).

327. The RP's approach to operating rules is based mainly on IAEA safety guide 'Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants' (Ref. 34).

5 CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

328. This report presents the findings of my assessment of the following cross-cutting topics of the generic UK HPR1000 safety case as part of the GDA process:

- Nuclear safety principles underpinning the UK HPR1000 reactor design and safety case.
- Development of the generic UK HPR1000 safety case.
- Management of commitments in the UK HPR1000 GDA.
- Management of implementable requirements and assumptions in the generic UK HPR1000 safety case.
- Approach to operating rules for UK HPR1000.
- Use of OPEX in the generic UK HPR1000 design and safety case.

329. Based on my assessment, undertaken on a sampling basis, I have concluded the following:

- The safety case for the above cross-cutting topics, which comprises the PCSR Chapters 4, 20 and 31 plus the supporting evidence, has been adequately developed for the purposes of GDA.
- The UK HPR1000 general safety and design principles are adequate for the purposes of GDA.
- The RP has established and deployed suitable means to deliver, in a timely manner, a comprehensive safety case.
- The RP has established adequate arrangements for capturing, managing and implementing commitments during GDA. The RP has identified and captured post-GDA commitments for the licensee to consider.
- The RP's process for identifying and tracing requirements through the generic UK HPR1000 safety case is adequate for the purposes of GDA. This process is at an early stage and it needs further development.
- The RP's approach for defining operating rules underpinned by the safety case is sufficient for GDA and suitable for further development by a licensee.
- The RP has developed adequate arrangements for identifying, capturing and analysing OPEX, including a suitable and sufficient new OPEX methodology.
- The RP's safety case for the above cross-cutting topics is aligned with ONR's SAPs, the relevant TAGs and with international good practice.
- As a result of my assessment, I have identified six Assessment Findings for the licensee to resolve.

330. 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 the perspective of the six cross-cutting topics covered in this report.

5.2 Recommendations

331. Based upon my assessment detailed in this report, I recommend that:

- **Recommendation 1**: From the perspective of the six cross-cutting topics considered in this report, ONR should grant a DAC for the generic UK HPR1000 design.

- **Recommendation 2**: The six 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. www.onr.org.uk/saps/saps2014.pdf
3. *ONR - Assessement of reactors - UK HPR1000 - Reports/Publications,* January 2022, ONR. www.onr.org.uk/new-reactors/uk-hpr1000/reports.htm
4. *Summary of the Step 4 Assessment of the UK HPR1000 Reactor. Project Assessment Report,* ONR-NR-PAR-21-001, Revision 0, January 2022, ONR. [CM9 Ref. 2021/37711]
5. *UK HPR1000 Pre-Construction Safety Report,* HPR/GDA/PCSR/0001 to 0033, Version 1, January 2020, GNSL. https://www.ukhpr1000.co.uk/documents-library/step-4/ [CM9 Ref. 5.1.3.10472]
6. *UK HPR1000 - Pre-Construction Safety Report Chapter 20 - MSQA and Safety Case Management,* GHX00620020KPGB02GN, Version 2 draft 1, June 2021, CGN. [CM9 Ref. 2021/48472]
7. *Pre-Construction Safety Report Chapter 31 Operational Management,* GHX00620031KPGB02GN, Version 2 draft 1, June 2021, CGN. [CM9 Ref. 2021/48459]
8. *Guidance on Mechanics of Assessment,* NS-TAST-GD-096, Revision 0, April 2020, ONR. [CM9 Ref. 2019/335774]
9. *GDA Regulatory Observation - Development of a Suitable and Sufficient Safety Case,* RO-UKHPR1000-0004, Revision 0, September 2018, ONR. www.onr.org.uk/new-reactors/uk-hpr1000/reports/ro-ukhpr1000-0004.pdf [CM9 Ref. 2018/255957]
10. *GDA Regulatory Observation – Identification and Use of OPEX in the UK HPR1000 Generic Design and Safety Case,,* RO-UKHPR1000-0044, Revision 0, May 2020, ONR. www.onr.org.uk/new-reactors/uk-hpr1000/reports/ro-ukhpr1000-0044.pdf [CM9 Ref. 2020/15072]
11. *UK HPR1000 - General Safety Requirements,* GHX00100017DOZJ03GN, Revision F, December 2019, CGN. [CM9 Ref. 2019/367630]
12. *UK HPR1000 - Regulatory Query (RQ) Tracking Sheet,* November 2017, ONR. [CM9 Ref. 2017/407871]
13. *UK HPR1000 - Safety Case Development Strategy,* HPR/GDA/REPO/0071, Revision 1, December 2019, GNSL. [CM9 Ref. 2019/367052]
14. *Management of Commitments for UK HPR1000 Generic Design Assessment (GDA) Project,* GH-40M-020, Revision C, May 2021, CGN. [CM9 Ref. 2021/43547]
15. *UK HPR1000 - Post-GDA Commitment List,* GHX00100084KPGB03GN, Revision B, June 2021, CGN. [CM9 Ref. 2021/0048119]
16. *Requirements Management Summary Report,* GHX00100127DOZJ03GN, Revision C, June 2021, CGN. [CM9 Ref. 2021/45082]
17. *Requirement Management Regulations for UK HPR1000 Generic Design Assessment (GDA) Project,* GH-40M-026, Revision C, May 2021, CGN. [CM9 Ref. 2021/43547]
18. *Generic Limits and Conditions for Normal Operation,* GHX37OTS001DOYX45GN, Revision B, May 2021, CGN. [CM9 Ref. 2021/37697]
19. *System OTS of Safety Injection System (RIS)[SIS] (The Translation Version of FCG Unit 3),* GHX36RISOTSDOYX45GN, Revision A, 2021 April, CGN. [CM9 Ref. 2021/37070]
20. *Management Rules on Experience Feedback of UK HPR1000 GDA Project,* GH-40M-001, Revision C, August 2020, CGN. [CM9 Ref. 2020/262040]

21. *Methodology for Use of OPEX in UK HPR1000,* GHX00100059DOZJ03GN, Revision A, August 2020, CGN. [CM9 Ref. 2020/260761]
22. *Regulatory Observations and Resolution Plans Website,* , ONR and Environment Agency. https://www.onr.org.uk/new-reactors/uk-hpr1000/ro-res-plan.htm
23. *Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable),* NS-TAST-GD-005, Revision 11, November 2020, ONR. www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-005.pdf
24. *Examination, Inspection, Maintenance and Testing of Items Important to Safety,* NS-TAST-GD-009, Revision 6, May 2019, ONR. www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-009.pdf
25. *Limits and Conditions For Nuclear Safety (Operating Rules),* NS-TAST-GD-035, Revision 6, March 2018, ONR. https://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-035.pdf
26. *Periodic Safety Reviews (PSR),* NS-TAST-GD-050, Revision 8, October 2020, ONR. www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-050.pdf
27. *The Purpose, Scope and Content of Saftey Cases,* NS-TAST-GD-051, Revision 7, December 2019, ONR. www.onr.org.uk/operational/tech_asst_guides/index.htm
28. *Fundamental Safety Principles,* Safety Standards Series No. SF-1, 2006, International Atomic Energy Agency (IAEA). www.iaea.org/publications/7592/fundamental-safety-principles
29. *Safety of Nuclear Power Plants: Design,* Safety Standards Series No. SSR-2/1, Revision 1, 2016, International Atomic Energy Agency (IAEA). www.iaea.org/publications/10885/safety-of-nuclear-power-plants-design
30. *Safety of Nuclear Power Plants: Commissioning and Operation Specific Safety Requirements,* Safety Standard Series No.SSR-2/2, Revision 1, 2016, International Atomic Energy Agency (IAEA). www-pub.iaea.org/MTCD/Publications/PDF/Pub1716web-18398071.pdf
31. *Safety Standards, Leadership and Management for Safety. General Safety Requirements,* Safety Standard Series No.GSR Part 2, 2016, International Atomic Energy Agency (IAEA). www-pub.iaea.org/MTCD/Publications/PDF/Pub1750web.pdf
32. *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-pub.iaea.org/MTCD/Publications/PDF/Pub1639_web.pdf
33. *Deterministic Safety Analysis for Nuclear Power,* Specific Safety Guide No. SSG-2, Revision 1, 2019, IAEA. www-pub.iaea.org/MTCD/Publications/PDF/PUB1851_web.pdf
34. *Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants,* Safety Guide NS-G-2.2, 2000, International Atomic Energy Agency (IAEA). www-pub.iaea.org/MTCD/publications/PDF/Pub1100_scr.pdf
35. *Safety of new Nuclear Power Plants (NPP) designs. WENRA Reactor Harmonization Working Group,* March 2013, Western European Nuclear Regulators' Association (WENRA). www.wenra.eu
36. *Safety Reference Levels for Existing Reactors 2020,* February 2021, Western European Nuclear Regulators' Association (WENRA). www.wenra.eu
37. *UK HPR1000 - Safety Case Development Manual,* HPR-GDA-REPO-0110, Revision 001, September 2020, GNSL. [CM9 Ref. 2020/268387]
38. *UK HPR1000 - Control of Service Provider Technical Work Procedure,* HPR/GDA/PROC/0028, Revision 1, January 2019, CGN. [CM9 Ref. CM9 2019/105515]
39. *UK HPR1000 - Management of Commitments for Safety Case Updates,* HPR-GDA-PROC-0046, Revision 4, July 2021, GNSL. [CM9 Ref. 2021/57087]

40. *New Nuclear Power Plants: Generic Design Assessment Technical Guidance,* ONR-GDA-GD-007, Revision 0, May 2019, ONR. www.onr.org.uk/new-reactors/reports/onr-gda-007.pdf
41. *UK HPR1000 - Pre-Construction Safety Report Chapter 4 General Safety and Design Principles,* HPR/GDA/PCSR/0004, Version 2, October 2021, GNSL. [CM9 Ref. 2021/72680]
42. *The Health and Safety at Work etc. Act 1974,* 1974, UK Goverment.
43. *Summary of the Step 3 Assessment of the UK HPR1000 Reactor,* ONR-NR-AR-19-001, Revision 1, February 2020, ONR. www.onr.org.uk/new-reactors/uk-hpr1000/reports/uk-hpr1000-step-3-summary-report.pdf [CM9 Ref. 2020/11336]
44. *Integrated Delivery Tool,* HPR/GDA/PROC/0142, Revision 0, May 2019, GNSL. [CM9 Ref. 2019/155668]
45. *UK HPR1000 Safety Case Delivery Management - Terms of Reference,* HPR-GDA-REPO-0081, Version 0, February 2019, GNSL. [CM9 Ref. 2019/59375]
46. *UK HPR1000 - Organisation and Operation Rules of UK HPR1000 GDA Project,* GH-40M-004, Revision C, May 2021, CGN. [CM9 Ref. 2021/39985]
47. *UK HPR1000 - Suitably Trained, Competent & Experienced Personnel – a Framework for GDA,* HPR/GDA/PROC/0029, Revision 0, October 2017, CGN. [CM9 Ref. 2019/105191]
48. *Position Training Guideline and Management Rules on Authorisation and Job Taking,* WD-EDE-060, Revision C, November 2018, CGN. [CM9 Ref. 2018/366711]
49. *Control of service provider technical work procedure,* HPR-GDA-PROC-0028, Revision A, July 2021, GNSL. [CM9 Ref. 2021/53786]
50. *MSQA Workshop / Inspection of GNSL,* ONR-NR-CR-20-407, Revision 0, July 2020, ONR. [CM9 Ref. 2020/252767]
51. *MSQA Workshop / Inspection of CGN,* ONR-NR-CR-20-724 , Revision 0, October 2020, ONR. [CM9 Ref. 2020/315112]
52. *Inspection of GDA MSQA arrangements in EDF,* ONR-NR-CR-20-1115 , Revision 0, February 2021, ONR. [CM9 Ref. 2021/0029748]
53. *UK HPR1000 - Safety Case & MSQA – Workshop,* ONR-NR-CR-21-203, Revision 0, July 2021, ONR. [CM9 Ref. 2021/54148]
54. *UK HPR1000 GDA - Safety Case Health Check - Summary Report,* ONR-NR-AN-20-005 , Revision 1, May 2020, ONR. [CM9 Ref. 2020/180830]
55. *Holistic ALARP Demonstration Report,* GHX00100071KPGB03GN, Revision C, June 2021, CGN. [CM9 Ref. 2021/50255]
56. *Safety Case Consolidation Strategy for UK HPR1000 GDA,* GHX00100085KPGB03GN, Revision A, March 2021, CGN. [CM9 Ref. 2021/28206]
57. *UK HPR1000 - GDA - Safety Case – Level 4 meeting,* ONR-NR-CR-21-055, Revision 0, April 2021, ONR. [CM9 Ref. 2021/37822]
58. *UK HPR1000 – GDA - Safety Case - Level 4 meeting,* ONR-NR-CR-21-165, Revision 0, June 2021, ONR. [CM9 Ref. 2021/48913]
59. *Safety Case Consolidation Summary Report,* GHX00100090KPGB03GN, Revision A, September 2021, CGN. [CM9 Ref. 2021/70730]
60. *UK HPR1000 - Pre-Construction Safety Report Chapter 20 MSQA and Safety Case Management,* HPR/GDA/PCSR/0020, Version 2, October 2021, GNSL. [CM9 Ref. 2021/72661]
61. *Assessment of the response to RO-UKHPR1000-0004 Development of a Suitable and Sufficient Safety Case,* ONR-NR-AN-21-040, Revision 0, October 2021, ONR. [CM9 Ref. 2021/48711]

62. *Step 4 Management for Safety and Quality Assurance Assessment of the UK HPR1000 Reactor,* ONR-NR-AR-21-003, Revision 0, January 2022, ONR. https://www.onr.org.uk/new-reactors/uk-hpr1000/reports.htm [CM9 Ref. 2021/42541]
63. *Requirement Management Report,* GHX00100122DOZJ03GN, Revision A, May 2019, CGN. [CM9 Ref. 2019/155661]
64. *UK HPR1000 Requirement Management Gap Analysis Report,* GHX00100125DOZJ03GN, Revision A, October 2019, CGN. [CM9 Ref. 2019/284302]
65. *UK HPR1000 - Lessons Learnt from Review Report of Requirement Management,* GHX00100091KPGB03GN, Revision A, August 2021, CGN. [CM9 Ref. 2021/61552]
66. *Assessment of the response to Action 4 of RO-UKHPR1000-0004 – Development of a Suitable and Sufficient Safety Case. Operational Examples,* ONR-NR-AN-21-042, Revision 0, August 2021, ONR. [CM9 Ref. 2021/57748]
67. *Assessment of the response to Action 4 of RO-UKHPR1000-0004 – Development of a Suitable and Sufficient Safety Case. Civil Engineering Examples,* ONR-NR-AN-21-039, Revision 0, August 2021, ONR. [CM9 Ref. 2021/55093]
68. *Assessment of the response to Action 4 of RO-UKHPR1000-0004 – Development of a Suitable and Sufficient Safety Case. Engineering Requirements,* ONR-NR-AN-21-037, Revision 0, August 2021, ONR. [CM9 Ref. 2021/63327]
69. *Step 4 Control & Instrumentation Assessment of the UK HPR1000 Reactor,* ONR-NR-AR-21-005, Revision 0, January 2022, ONR. https://www.onr.org.uk/new-reactors/uk-hpr1000/reports.htm [CM9 Ref. 2021/46296]
70. *Step 4 Assessment of Fuel and Core for the UK HPR1000 Reactor,* ONR-NR-AR-21-021, Revision 0, January 2022, ONR. https://www.onr.org.uk/new-reactors/uk-hpr1000/reports.htm [CM9 Ref. 2021/23724]
71. *Step 4 Mechanical Engineering Assessment Report,* ONR-NR-AR-21-004, Revision 0, January 2022, ONR. https://www.onr.org.uk/new-reactors/uk-hpr1000/reports.htm [CM9 Ref. 2021/53696]
72. *Step 4 Decommissioning Assessment of the UK HPR1000 Reactor,* ONR-NR-AR-21-015, Revision 0, January 2022, ONR. https://www.onr.org.uk/new-reactors/uk-hpr1000/reports.htm [CM9 Ref. 2021/51023]
73. *UK HPR1000 – Safety Case Meeting – RO-0004 Requirements Management – Layouts,* ONR-NR-CR-20-399, Revision 0, August 2020, ONR. [CM9 Ref. 2020/251352]
74. *UK HPR1000 - Generic Design Assessment – Cross Cutting – 3D Model Level 4 Meeting,* ONR-NR-CR-20-807, Revision 0, December 2020, ONR. [CM9 Ref. 2020/323262]
75. *Periodic Test Completeness Note of Safety Injection System (RIS),* GHX39RIS001DNHX45SS, Revision D, June 2021, CGN. [CM9 Ref. 2021/52398]
76. *System Commissioning Program of Safety Injection System (RIS),* GHX26RISC01DNHX45SS, Revision C, May 2021, CGN. [CM9 Ref. 2021/43579]
77. *Examination, Maintenance, Inspection and Testing (EMIT) Windows,* GHX42EMT002DOYX45GN, Revision D, January 2021, CGN. [CM9 Ref. 2021/8441]
78. *Assessment of the approach to Operating Rules for UK HPR1000 during GDA,* ONR-NR-AN-21-041, Revision 0, September 2021, ONR. [CM9 Ref. 2021/68080]
79. *Generic Water Chemistry Specification (LCO),* GHX00100101DCHS03GN, Revision E, May 2021, CGN. [CM9 Ref. 2021/43591]
80. *Operating Technical Specifications Methodology,* NE15BWXYX0000000012, Revision B, September 2018, CGN. [CM9 Ref. 2018/315855]
81. *UK HPR1000 Fault Schedule,* GHX00600276DRAF02GN , Revision D, January 2021, CGN. [CM9 Ref. 2021/8482]

82. *RIS-Safety Injection System Design Manual Chapter 3 System Functions and Design Bases,* GHX17RIS003DNHX45GN, Revision F, May 2021, CGN. [CM9 Ref. 2021/43575]
83. *Technical Specifications, 10 CFR 50.36,* June 2021, US NRC. www.nrc.gov
84. *Step 4 Assessment of Structural Integrity for the UK HPR1000 Reactor,* ONR-NR-AR-21-016, Revision 0, 2021, ONR. [CM9 Ref. 2021/52300]
85. *UK HPR1000 - Pre-Construction Safety Report,* HPR/GDA/PCSR/0001 to HPR/GDA/PCSR/0033, Version 2, September 2021, GNSL. [CM9 Ref. 4.4.1.4421]
86. *Principle and Content of Ageing Management Programme,* GHX37AMP001SPNS45GN, Revision A, November 2020, CGN. [CM9 Ref. 2020/322758]
87. *UK HPR1000 - Pre-Construction Safety Report Chapter 31 Operational Management,* HPR/GDA/PCSR/0031, Version 2, October 2021, GNSL. [CM9 Ref. 2021/72617]
88. *Assessment of the Response to RO-UKHPR1000-0044 – Identification and Use of OPEX in the UK HPR1000 Generic Design and Safety Case,* ONR-NR-AN-21-012, Revision 0, May 2021, ONR. [CM9 Ref. 2021/37941]
89. *Sample Submission Programme for OPEX-Dependent Topics,* GHX35000001DMGL03GN, Revision A, October 2020, CGN. [CM9 Ref. 2020/305478]
90. *UK HPR1000 - Pre-Construction Safety Report Chapter 4 - General Safety and Design Principles,* GHX00620004KPGB02GN, Version 2 Draft 1, June 2021, CGN. [CM9 Ref. 2021/48488]
91. *UK HPR1000 Design Reference Report,* NE15BW-X-GL-0000-000047, Revision H, July 2021, CGN. [CM9 Ref. 2021/58832]
92. *Generic limits and conditions of operation - Response,* RQ-UKHPR1000-1681 , Revision 0, April 2021, GNSL. [CM9 Ref. 2021/33731]
93. *Safety Functional Requirements of RIS [SIS],* GHX00600351DRAF02GN, Revision E, May 2021, CGN. [CM9 Ref. 2021/43560]
94. *UK HPR1000 Fault Schedule,* GHX00600276DRAF02GN, Revision E, August 2021, CGN. [CM9 Ref. 2021/64934]
95. *RIS-Safety Injection System Design Manual Chapter 4 System and Component Design,* GHX17RIS004DNHX45GN, Revision F, July 2021, CGN. [CM9 Ref. 2021/52389]
96. *Engineering Schedule for Mechanical Engineering,* GHX00100027DNHX03GN, Revision F, May 2021, CGN. [CM9 Ref. 2021/43585]
97. *Extant Duty Schedule of RIS [SIS]/ASG [EFWS]/DCL [MCRACS],* GHX11000003DOZJ45GN, Revision B, June 2021, CGN. [CM9 Ref. 2021/44502]
98. *RIS-Safety Injection System Design Manual Chapter 6 System Operation and Maintenance,* GHX17RIS006DNHX45GN, Revision G, May 2021, CGN. [CM9 Ref. 2021/43577]
99. *Pre-service Inspection List of Safety Injection System (RIS),* GHX99RIS002DNHX45GN, Revision A, October 2019, CGN. [CM9 Ref. 2019/318767]
100. *PTR-Fuel Pool Cooling and Treatment System Design Manual Chapter 3 System Functions and Design Bases,* GHX17PTR003DNHX45GN, Revision G, July 2021, CGN. [CM9 Ref. 2021/52337]
101. *Allocation of Function Review Report,* GHX00100011DIKX03GN, Revision B, March 2021, CGN. [CM9 Ref. 2021/27274]
102. *UK HPR1000 - Basis of Safety Case for BFX,* GHXFXX10001DWJG42GN, Revision K, May 2021, CGN. [CM9 Ref. 2021/43603]
103. *UK HPR1000 - Design substantiation report for BFX,* GHXFXX10004DWJG42GN, Revision C, May 2021, CGN. [CM9 Ref. 2021/43604]
104. *UK HPR1000 - Construction and testing report,* GHXNIX10031DWJG42GN, Revision B, May 2021, CGN. [CM9 Ref. 2021/37704]

105. *Civil Engineering Schedule Report,* GHXNIX10058DWJG42GN, Revision B, July 2021, CGN. [CM9 Ref. 2021/56418]
106. *UK HPR1000 - Basis of design for BFX,* GHXFXX10002DWJG42GN, Revision H, July 2021, CGN. [CM9 Ref. 2021/55230]
107. *UK HPR1000 - GHX00100033DNFP03GN - Fuel Building Shielding Design Report,* Revision E, April 2021, CGN. [CM9 Ref. 2021/36843]
108. *UK HPR1000 - Internal Hazards Schedule Report,* GHX84200051DOZJ03GN, Revision C, April 2021, CGN. [CM9 Ref. 2021/30052]
109. *UK HPR1000 - High Energy Pipe Failures Safety Assessment Report for Fuel Building.,* GHX84200047DOZJ03GN , Revision A, October 2020, CGN. [CM9 Ref. 2020/304805]
110. *UK HPR1000 - Reinforced concrete barrier substantiation report for BFX,* GHXFXX10005DWJG42GN, Revision F, July 2021, CGN. [CM9 Ref. 2021/55244]
111. *UK HPR1000 - External Hazards Schedule Report,* GHX86000015DOZJ03GN , Revision G, May 2021, CGN. [CM9 Ref. 2021/43513]
112. *UK HPR1000 - Aircraft Crash Safety Evaluation Report,* GHX86000016DOZJ03GN, Revision C, June 2021, CGN. [CM9 Ref. 2021/50558]
113. *UK HPR1000 - Generic Site Related Design Values,* GHX00100007DOZJ03GN, Revision D, January 2021, CGN. [CM9 Ref. 2021/4287]
114. *UK HPR1000 - Structural analysis and design report for BFX,* GHXFXX10003DWJG42GN, Revision E, July 2021, CGN. [CM9 Ref. 2021/55238]

Annex 1

Relevant Safety Assessment Principles Considered During the Assessment

SAP No	SAP Title	Description
MS.4	**Leadership and management for safety** Learning	Lessons should be learned from internal and external sources to continually improve leadership, organisational capability, the management system, safety decision making and safety performance
SC.1	**The regulatory assessment of safety cases** Safety case production process	The process for producing safety cases should be designed and operated commensurate with the hazard, using concepts applied to high reliability engineered systems.
SC.2	**The regulatory assessment of safety cases** Safety case process outputs	The safety case process should produce safety cases that facilitate safe operation.
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.6	**The regulatory assessment of safety cases** Safety case content and implementation	The safety case for a facility or site should identify the important aspects of operation and management required for maintaining safety and how these will be implemented.
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.
SC.8	**The regulatory assessment of safety cases** Safety case ownership	Ownership of the safety case should reside within the dutyholder's organisation with those who have direct responsibility for safety.
ECS.3	**Engineering principles: key principles** 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.
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.

SAP No	SAP Title	Description
ECE.12	**Engineering principles: civil engineering: structural analysis and model testing** Structural analysis and model testing	Structural analysis and/or model testing should be carried out to support the design and should demonstrate that the structure can fulfil its safety functional requirements over the full range of loading for the lifetime of the facility.
ECV.2	**Engineering principles: containment and ventilation: containment design** Minimisation of releases	Containment and associated systems should be designed to minimise radioactive releases to the environment in normal operation, fault and accident conditions.
ECV.3	**Engineering principles: containment and ventilation: containment design** Means of confinement	The primary means of confining radioactive materials should be through the provision of passive sealed containment systems and intrinsic safety features, in preference to the use of active dynamic systems and components.

Note: For my assessment of the RP's NSPs I have considered all SAPs (Ref. 2)

Annex 2

Assessment Findings

Number	Assessment Finding	Report Section
AF-UKHPR1000-0106	The licensee shall develop nuclear safety principles to underpin all aspects of the design and the lifecycle of the nuclear facility. These should include resolving the shortfalls identified during GDA.	4.2.3
AF-UKHPR1000-0107	The licensee shall, in implementing its chosen process to manage requirements identified within the safety case, demonstrate the scope captures all necessary aspects of the safety case. This should include resolving the related shortfalls identified during GDA of: ■ Ensuring that all systems, structures and components that are required to fulfil a safety function or can affect the successful fulfilment of a safety function, are subject to the process. ■ Ensuring full traceability of the engineering performance requirements for systems, structures and components that fulfil a safety function. ■ Demonstrating that the process can be applied to human factors-related requirements, including consideration of the definitions, granularity and clarity of human factors-related requirements, in addition to how it is applied to the underlying analysis. ■ Demonstrating that the process can be applied to inspection-related requirements. ■ Ensuring the traceability of non-codified requirements through the safety case.	4.5.1.4

Number	Assessment Finding	Report Section
AF-UKHPR1000-0108	The licensee shall, in implementing its chosen process to manage requirements identified within the safety case, demonstrate that it can identify their source and traceability to provide their underpinning within the safety case. This should include resolving the specific shortfalls identified during GDA of: ■ Ensuring traceability is bidirectional, from the source of the requirement to the design, analysis or operational documentation and vice versa. ■ Providing sufficient references to allow traceability, including for non-codified requirements. ■ Improving the linkages between the different documents, including schedules, and in particular where requirements are transferred between documents. ■ Ensuring commissioning and operational aspects can be traced sufficiently and in particular to the documents demonstrating fulfilment of each specific safety function.	4.5.1.4
AF-UKHPR1000-0109	The licensee shall, in implementing its chosen process to manage requirements identified within the safety case, demonstrate that it is undertaken to an adequate level of detail. The definition and decomposition of functions should be consistent, clear, traceable and to a level of granularity that is sufficient to implement the management of identified requirements.	4.5.1.4

Number	Assessment Finding	Report Section
AF-UKHPR1000-0110	The licensee shall, in implementing its chosen process to manage requirements identified from the safety case, enhance the requirements management process demonstrated during GDA by: ■ Providing additional guidance over the interface and overlap between fault, duty and other functional requirements and their definition in terms of the categorisation of the safety functions. ■ Providing additional guidance on the grouping of individual functions to ensure traceability, including the use of function groups, complex functions and three-field codes. ■ Avoiding the mixing of passive, active, manual and automatic functions in function groups where it is not appropriate to do so. ■ Clarifying the use of engineering requirements identifiers and item codes to aid with traceability. ■ Including guidance on traceability of non-codified requirements. ■ Ensuring that adequate verification activities are included in the process to ensure correctness and alignment across the suite of safety case and design documents.	4.5.1.4
AF-UKHPR1000-0111	The licensee shall, as part of implementing site specific operating rules, ensure that the approach includes all important aspects of operation and management, in view of the type and magnitude of hazards involved. This should include those aspects not fully developed during GDA including identified hazards, all levels of defence in depth and human related claims.	4.6.1.2

Annex 3

List of Cross-cutting Topics

Number	Cross-cutting Topics	Reported in*
1.	Development of the generic UK HPR1000 safety case	This assessment report
2.	Demonstration that the risks in the UK HPR1000 design have been reduced to ALARP – 'ALARP Demonstration' & Holistic ALARP	Summary Report Topic Specific Assessment Reports
3.	Nuclear safety principles underpinning the generic UK HPR1000 design and safety case	This assessment report
4.	Scope of the UK HPR1000 GDA	Summary Report
5.	Design Control – Design Reference, Master Document Submission List and design changes.	Topic Specific Assessment Reports Summary Report
6.	Management of safety case commitments, requirements and assumptions in the generic UK HPR1000 safety case	This assessment report
7.	Categorisation of safety functions & classification of safety measures	Topic Specific Assessment Reports
8.	Approach to operating rules for UK HPR1000	This assessment report
9.	Comparison against the numerical targets in ONR's SAPs	Topic Specific Assessment Reports
10.	Adequacy of the safety case for the UK HPR1000 fuel route in the Fuel Building	Topic Specific Assessment Reports
11.	Security and safety interactions	Topic Specific Assessment Reports
12.	Demonstration of the defence-in-depth and diversity in the UK HPR1000 design	Topic Specific Assessment Reports
13.	Approach to Examination, Maintenance, Inspection & Testing (EMIT) for the UK HPR1000	Topic Specific Assessment Reports
14.	Adequacy of the Spent Fuel Interim Storage (SFIS) facility safety case	Topic Specific Assessment Reports
15.	Radioactive waste safety case for the UK HPR1000	Topic Specific Assessment Reports
16.	Holistic assessment of the Heating, Ventilation and Air Conditioning (HVAC) system	Topic Specific Assessment Reports
17.	Use of Operating Experience in the generic UK HPR1000 design and safety case	This assessment report
18.	Source term assessment for normal operations and fault / accident conditions	Topic Specific Assessment Reports
19.	Assessment of the generic UK HPR1000 design against space weather hazards	Topic Specific Assessment Reports

Number	Cross-cutting Topics	Reported in*
20.	Cyber security	Topic Specific Assessment Reports
21.	Overview of ONR's assessment of the generic UK HPR1000 layout design	Topic Specific Assessment Reports
22.	Grid Code compliance of the generic UK HPR1000 design	Topic Specific Assessment Reports

*Note: All ONR's UK HPR1000 GDA reports can be found on the GDA joint regulators' website (Ref. 3).

Annex 4

Safety Case Requirements Management – Examples

332. The requirements management process described in sub-section 4.5 was applied retrospectively by the RP to a sample of systems and structures to demonstrate the suitability of its arrangements. In order to sample the traceability of requirements through the safety case, I selected the examples in the Table 2, which provides the examples of systems, structures and the requirements sampled.

Table 2: Examples of systems, structures and requirements sampled

Number	Example Description	Requirements Sampled
1	The demonstration of full traceability for the full set of engineering and operational requirements and assumptions for the RIS [SIS]	a) RIS-FFR-02 – Injection of accumulator b) RIG-FFR-01-A11 – Reactor coolant pressure boundary isolation c) RIS-FFR-07-M41 – Low head safety injection in cold leg d) RIS-FFR-012-A11 – Reactor coolant pressure boundary isolation
2	The demonstration of full traceability for the operational and engineering requirements and assumptions associated with the cooling functions of the RIS [SIS].	a) RIS-OFR-02 – Residual Heat Removal (RHR) start-up under normal shutdown conditions b) RIS-OFR-05 Temperature control of primary loop after RHR connection c) RIS-OFR-06 - RHR Flowrate control
3	The demonstration of full traceability for the operational and engineering requirements and assumptions associated with the clean-up functions of the PTR [FPCTS]	a) PTR-OFR-02 – Purification of the fuel building pools (SFP, transfer compartment and cask loading pit) b) Boron control in the SFP
4	The demonstration of full traceability for a set of human factors requirements of the RIS [SIS].	a) RIS-FFR-01-M41 – Connection and start-up of RIS/RHR b) RIS-FFR-07-M41 – Low head safety injection in cold leg c) RIS-FFR-13-M41 – Simultaneous injection in cold leg and hot leg d) RIS-FFR-18-M11 – Manual block of isolation of RIS/RHR train (reactor pool level low 1 in state E)
5	The demonstration of full traceability for a set of constructability requirements and assumptions for the SFP liner	Constructability requirements associated with SFP – The requirements are not codified

Number	Example Description	Requirements Sampled
6	The demonstration of full traceability for a set of shielding requirements and assumptions for the BFX	Shielding requirements are not codified at the civil engineering schedule entry point. I have traced the requirement through the civil engineering documents with engineering IDs: BFX-01-01-05 & BFX-02-01-03
7	The demonstration of full traceability for a set of in-service inspection and leak detection requirements and assumptions for the SFP and IRWST	PTR-OFR-24 - Leakage detection of the pools
8	The demonstration of full traceability for a set of high energy pipe failure requirements and assumptions for the BFX.	a) BFX-IHE-02-P01 – High energy pipe failure b) BFX-IHE-07-P01 – High energy pipe failure c) BFX-ICH-01-P01 – Combined hazards
9	The demonstration of full traceability for a set of aircraft impact requirements and assumptions for the BFX.	a) EH-AC-BFX-01 – Design basis aircraft load b) EH-AC-BFX-02 – Beyond design basis aircraft load c) EH-AC-BFX-03 – Beyond design basis aircraft load
10	The demonstration of full traceability for a set of requirements and assumptions for a PIE that results in a temperature and pressure challenge to the SFP.	Temperature and pressure requirements are not codified at the civil engineering schedule entry point. I have traced the requirements through the civil engineering documents with engineering IDs: BFX-02-01-01 and BFX-02-01-02

333. I have carried out my assessment by tracing requirement using the coding system if such a coding system was available. I reflected this in Table 2 under the samples' column. However, there are two main limitations to this approach which I explain below.

334. The first limitation is that the RP's requirement management process limits the scope of the coding system to a core suite of documentation where the main aspects of the design process intersect. This includes the various schedules, requirement reports, design and operational documents. An artifact of this approach is that many of the specific requirements originate in documentation outside of this core suite. This creates a risk that the traceability of requirements is lost. The RP also makes use of the unique item codes that apply to components. These item codes already exist as part of the design. Therefore, it is relevant to note that I have identified some of the requirements through the item code, rather than the requirement management coding.

335. The second limitation is the traceability of non-codified requirements. Therefore, in order to trace non-codified requirements, I relied on referencing, engineering IDs and on understanding the structure of the safety case.

336. I have summarised the outcome of my assessment for each of the examples below.

Example 1 – Engineering and Operational Requirements for the Safety Injection System RIS [SIS]

337. Example 1 was intended to be the 'full scope' example provided by the RP to demonstrate the breadth and depth of application of its requirements management process. I sampled a number of fault functional requirements (mainly RIS-FFR-07-M41 and RIS-FFR-012-A11), but I focused on the fault functional requirement RIS-FFR-02, which is associated with 'injection of accumulator' and it is a category 1 safety function.

338. In my assessment I identified multiple functions against the three-field code, RIS-FFR-02, including those associated with control of reactivity, removal of heat and an incorrect citation against filtration. However, the three-field text was not specific enough to identify precisely the safety function. After I raised this, the RP removed the ambiguity from the safety case, but it also removed one safety function (removal of heat) which is referred in a number of reports, such as the 'Safety Functional Requirements Report (SFRR) of the RIS [SIS]' (Ref. 93). This is an inconsistency that is not surprising given that this is a new process to the RP. However, it highlights the allocation of multiple Fault Functional Requirements (FFRs) against three-field safety functions. The RP explained that different FFRs could apply under different conditions to fulfil the safety function. Nonetheless, there is no immediate or obvious mechanism in the documentation to identify where this is applied, nor decompose it when necessary. I also consider this to be a matter that hinders traceability.

339. The RP introduced the concept of function groups in the fault schedule (Ref. 81) where several functions are grouped and implemented together to achieve one 'complex function'. This concept was not part of the procedure (Ref. 17) or the summary report (Ref. 16) but was added later as result of one of my RQs. It should be noted that the definition of complex function is still not present in the RP's procedure and summary report.

340. The main shortfall that I found with function groups was regarding traceability. Some of those function groups contained 17 individual functions across 17 different systems and, whilst I can see the benefit in such an approach, in terms of identification of requirements, it remains necessary to identify and code the individual functions. Also, in some cases the RP grouped separate functions which had different associated requirements. Furthermore, during my assessment I found that the source of the requirements for the RIS [SIS} (Ref. 93) did not contain the individual coding for the functions within a function group. Again, I consider that the lack of the individual coding hinders traceability and reinforces the need for further clarity on the approach to grouping of functions.

341. I also noted that RIG-FFR-01-A11 does not conform with the requirements management rule of avoiding mixing active and passive functions within a group. The RP addressed this particular shortfall in the updated fault schedule (Ref. 94). It should be noted that the definition of active function is not in the procedure or summary report.

342. I judge that further consideration needs to be given to abbreviated functions (three-fields), function groups, complex functions and mixing active and passive functions. I consider this to be a shortfall regarding the requirements management process and so I have consolidated all process related shortfalls under Assessment Finding AF-UKHPR1000-0110 (see Annex 2).

343. In this particular example, I noted that the use of leading zeroes in the third field of function codes hinders traceability and was not consistent with the RP's requirements management procedure (Ref. 17) or the summary report (Ref. 16). I consider this to be a minor shortfall and the licensee may consider this improvement as part of the development of the requirements management arrangements.

344. In terms of identification of the requirement, I identified in the engineering and operational documentation the FFR, RIS-FFR-02, and therefore I am content that can be identified from the various documents.

345. In terms of traceability, I traced RIS-FFR-02 through the SFRR (Ref. 93) and fault schedule (Ref. 81). However, the specific requirements, for example the values for accumulator volume or pressure, are not given in the referenced analysis and there is no use of the functional coding in the transient analysis. This traceability is therefore one-directional. I consider this to be a weakness in the requirements management arrangements and traceability of functional requirements. I found the same shortfall in several examples (see below), and so I consider this to be a matter that must be resolved by the licensee. I have captured all traceability shortfalls in Assessment Finding AF-UKHPR1000-0108 (see Annex 2).

346. Further engineering performance requirements for the functions sampled in this example could be found in the SDMs Chapters 3 and 4 (Ref. 82, Ref. 95). I queried the RP on the source of these requirements and the RP clarified that these were based on the Fangchenggang NPP Unit 3 design and 'Equipment Design Process Reports' that provide the underpinning for design-based requirements. Those reports have not been submitted in GDA, and whilst I acknowledge that the performance requirements will be developed during the detailed design phase, the source of the requirements should be identified. Therefore, I consider that the licensee needs to provide full traceability of the engineering performance requirements for SSCs that fulfil safety functions.

347. The lack of bidirectional traceability and the shortfalls on the identification of the source of the engineering performance requirements are shortfalls regarding traceability. As indicated above, I have captured all the shortfalls regarding traceability under Assessment Finding AF-UKHPR1000-0108.

348. The operational and commissioning aspects are given in the 'Periodic Test Completeness Note (PTCN)' (Ref. 75), 'System Commissioning Programme' (Ref. 76) and 'EMIT Windows' report (Ref. 77). These documents contain the requirements management coding, and traceability is therefore simple. However, there are several differences between the information presented in these more detailed operational documents and elsewhere, as it seems to be additional operational requirements associated with RIS-FFR-02. For example, the 'System Commissioning Programme' (Ref. 76) identifies specific tests associated with the three-field code (RIS-FFR-02), but the three-field code does not provide the granularity needed, as there are a number of specific safety functions associated with this code. The RP stated that much of the operational and commissioning information will be developed post-GDA. I am content that sufficient was provided to meet the intent of a demonstration for GDA, but this needs further consideration as the detailed design develops and the requirements management process is applied more widely. I consider this to be a shortfall regarding traceability that needs resolving after GDA, and I have captured it under Assessment Finding AF-UKHPR1000-0108, which also covers the traceability of commissioning and operational aspects.

349. The 'EMIT Windows' report (Ref. 77) contains a significant number of equipment that is not mentioned in the mechanical engineering schedule (Ref. 96) against specific safety functions. The RP identifies this equipment as 'non-typical component of a safety feature' which means "component which does not directly deliver the safety feature but

has impact on the performance of this safety feature". Whilst I understand that the 'non-typical components' will be part of the detailed design and the RP has provided enough evidence for GDA, those components need to be included into the requirements management process. I consider this to be a scope shortfall that needs to be resolved by the licensee and should be tracked by ONR. I have consolidated all the requirements management shortfalls regarding scope under a single Assessment Finding AF-UKHPR1000-0107 (See Annex 2).

350. In general, this example highlighted that the definition and granularity of the functions and the resulting requirements, as currently presented, are not detailed or specific enough. Whilst the lack of granularity is understandable given the level of maturity of the GDA design, this is an area that the licensee needs to develop further, and so I have raised an Assessment Finding AF-UKHPR1000-0109 (see Annex 2).

Example 2 - Operational and Engineering Requirements and Assumptions Associated with the Cooling Functions of the Safety Injection System RIS [SIS]

351. For this implementation example provided by the RP, I chose to sample several 'Other Functional Requirements' (OFR) associated with the use of the RIS [SIS] system in RHR mode. More specifically these were RIS-OFR-02, 05 and 06 associated with RHR start-up under normal shutdown conditions, temperature control of primary loop after RHR connection, and RHR flowrate control, respectively. These are identified by the RP as category 2 functions.

352. As result of one of my RQs, the RP changed these OFRs to Duty Functional Requirements (DFR), covered under RIS-DFR-01. This was further evidence of how the requirements management process was evolving as it was applied, and a licensee will need to consider and refine the classification of requirements before it is applied more widely. I consider this to be a shortfall in the process and I have captured this under Assessment Finding AF-UKHPR1000-0110, which, as already explained, covers the shortfalls on the requirements management process.

353. During my assessment, I also noted that for C&I the RP grouped together functions which have different associated requirements (in other words mixing DFRs and OFRs). However, the requirements management process offers little specific guidance in terms of grouping of functions or what constitutes a complex function. The lack of guidance on function groups is a process matter and I have therefore captured it under Assessment Finding AF-UKHPR1000-0110.

354. In terms of identification of requirements, I identified specific requirements associated with DFR RIS-DFR-01 in a range of design and operational documents. However, identifying the specific requirements associated with this DFR was not straightforward, partly due to the RP's decision to group a number of functions and partly due to the wide range of documents involved.

355. In terms of traceability, requirement RIS-DFR- 01 was identified and coded in the duty schedule (Ref. 97), then transferred to the SSCs design at the equipment level via the SDM chapters, and summarised in the mechanical engineering schedule (Ref. 96). Operational requirements were recorded in SDM Chapter 6 (Ref. 98) and the RIS [SIS] pre-service inspection list (Ref. 99). The RP noted that many of the detailed requirements for RIS-DFR-01 will be transferred through function code or item code in the post-GDA stage for matters such as detailed equipment design and manufacture, operational aspects, ISI, and commissioning requirements. I consider that the combination of applied requirement management coding and existing item codes provides a reasonable mechanism to trace the requirements.

356. Overall, I consider that, for this example, the RP provided a suitable demonstration of the requirement management application and confidence that it could be further developed by a licensee.

Example 3 - Operational and Engineering Requirements and Assumptions Associated with the Clean-up Functions of the Fuel Pool Cooling and Treatment System PTR [FPCTS]

357. I chose to sample the OFR PTR-OFR-02 - purification of the fuel building pools (SFP, transfer compartment and cask loading pit). I identified the specific requirements associated with this function in multiple documents, and RP's responses to RQs triggered improvements in the identification of chemistry related requirements. I identified some inconsistencies, in terms of safety classification, but overall, I am satisfied that the RP identified the main requirements. This is consistent with the expectation in SAP EMT.1 on identification of requirements.

358. In terms of traceability, I am content with the traceability of requirement PTR-OFR-02 through the safety case, although there is limited information for the operational requirements. The RP stated that detailed EMIT requirement will be transferred to the associated documents in site-specific stages through the item codes. This will allow the detailed design and manufacturing requirements, operating rules and test procedures to be developed. As with the other examples assessed, this appears to be a reasonable approach but lacks the details necessary for a demonstration during GDA. The traceability of the operational requirements is captured under Assessment Finding AF-UKHPR1000-0108.

359. I also assessed the boron control in the SFP, where I noted an anomaly in how the RP had identified functions. I realised that one of the safety functions identified in the PTR [FPCTS] SDM Chapter 3 (Ref. 100) was not codified (unlike all the others in the SDM). The RP updated the report but changed this function to a 'duty function'. Whilst I am content with the change, it reinforces the Assessment Finding AF-UKHPR1000-0110 related to the requirements management process. The traceability of the boron control in the SFP is similar to the other examples where the core suite of design documents (SDMs etc.) uses the coding to assure traceability, and this is further decomposed to the item code for onward linkage to detailed operational documents (post-GDA). I am content with the traceability of the boron control in the SFP for GDA.

Example 4 - Human Factors Requirements of the Safety Injection System RIS [SIS]

360. I chose to sample aspects of the implementation of human factors requirements, associated with the RIS [SIS]. The 'Requirements Management Summary Report' (Ref. 16) explains that CGN's design process for the UK HPR1000 project was enhanced to include human factors within the design assessment process, which is positive. The 'Requirements Management Summary Report' (Ref. 16) also provides an appendix outlining the four manual actions which I chose as my sample. Many documents listed in this appendix contain, according to the RP, general and specific human factors requirements. I sampled these documents, and I found the following:

- The most detailed documents identified by the RP are the 'Allocation of Function Review Report' (Ref. 101) and the subsequent Human Based Safety Claim (HBSC) reviews. I sampled four functions (see Table 2 above) but the HBSC assessment did not assign specific human factors requirements to those functions.
- The information in the RP's requirements management approach and procedure (Ref. 16, Ref. 17) does not include any aspects related to operational matters.

- I identified human factors assumptions, but the requirements management coding is not applied to those.

361. Therefore, I consider the requirements identified to be largely generic in nature, with none that I would consider to be specific as per the RP's process.

362. Overall, on the basis of my assessment of this example, I was unable to identify or trace any specific requirements associated with human factors on the RIS [SIS]. I therefore judge that the RP has not demonstrated that its requirements management process is adequate, or can be applied, to human factors related requirements. While I accept that this is more difficult to do during GDA, and the RP has worked to integrate human factors into the design process more generally, this will need to be an area of particular focus for the licensee as the requirements management process is applied more widely during the detailed design and site-specific stages. I consider improvements to the definitions, granularity and clarity of human factors related requirements is needed, in addition to how it is applied to assumptions. I consider this to be a shortfall on the scope of the requirements management, and so I have captured it under Assessment Finding AF-UKHPR1000-0107 related to requirements management scope.

Example 5 – Constructability Requirements and Assumptions for the Spent Fuel Pool Liner

363. I chose to sample the constructability requirements and assumptions associated with the SFP, and in particular the liner.

364. I sampled the Basis of Safety Case (BoSC) (Ref. 102) and the Design Substantiation Report (DSR) for the BFX (Ref. 103). These two reports provide a route map of the documents comprising the civil engineering safety case. One of these reports is the 'Construction and Testing Report' (Ref. 104), which contains construction requirements for the BRX, general construction requirements and a short section on the construction of the SFP liner. The majority of the requirements are general requirements, but there are some that could be classified as specific. The construction requirements in the 'Construction and Testing Report' (Ref. 104) are not codified but the route map provided in the BoSC allowed me to identify and trace those requirements.

365. In GDA, the constructability aspects are covered at a very high level, and the majority are general requirements. From the perspective of Civil Engineering, the construction requirements in GDA can be identified and traced, however, during the site-specific stages, and as the level of interfaces increases, the current arrangements will need further development to include the traceability of non-codified requirements and assumptions through the safety case. Traceability of non-codified requirements is not part of the requirements management process. I consider this to be a shortfall in terms of scope and I have therefore captured this under Assessment Finding AF-UKHPR1000-0107.

Example 6 - Shielding Requirements and Assumptions for the Fuel Building

366. I chose to sample the shielding requirements and assumptions associated with the BFX.

367. The shielding requirements do not have a requirements management code, but they can be identified through the civil engineering schedule (Ref. 105), the BoSC (Ref. 102) and the DSR (Ref. 106) for the BFX. All three documents refer to the upstream reference 'Fuel Building Shielding Design Report' (Ref. 107) that identifies the shielding requirements.

368. In terms of traceability, the shielding requirements can be traced from the BoSC to the DSR through the engineering requirement IDs, but this is not explained in the RP's requirements management approach and procedure (Ref. 16, Ref. 17). I consider this to be a shortfall with the requirements management process and so I have captured it under Assessment Finding AF-UKHPR1000-0110.

369. I sampled the BFX shielding report (Ref. 107) which is the upstream reference or source of the requirement. This report contains specific shielding requirements, for example the wall thicknesses, but those are non-codified specific requirements and the shielding report (Ref. 107) does not reference the civil engineering reports. Without the coding or references, I could not trace the requirements back to the civil engineering schedule, the BoSC or the DSR. Therefore, the traceability is one-directional. I found the same matter in example 1, and as stated there, I consider this to be a shortfall in the requirements management arrangements and traceability of functions. Therefore, I have captured this under Assessment Finding AF-UKHPR1000-0108 related to traceability of requirements.

Example 7 - In-service Inspection and Leak Detection Requirements and Assumptions for the Spent Fuel Pool and the In-containment Refuelling Water Storage Tank

370. In my opinion, the RP did not provide specific ISI requirements for the SFP and the IRWST:

- I sampled PTR-OFR-24 (leakage detection of the pools - SFP) and raised an RQ on this, but despite the updates, and the obvious enhancements made to some of the key submissions to incorporate this OFR, I was not able to identify several requirements that I expected to find. Notably, I was unable to find the allowable leak rate for the SFP.
- As a response to one of my RQs, the RP identified RIS-OFR-22 in relation to leak detection from the IRWST. However, there is no requirements associated with this function other than the requirement for leak tightness of the liner.

371. The RP stated that at this stage in GDA only general requirements for ISI have been identified. Specific ISI requirements will be identified in detailed design and included in the pre-service and ISI programmes and the technical specifications.

372. In terms of identification of requirements, the RP has not adequately demonstrated the requirements management process for the SFP and the IRWST. However, the RP provided a further example for the accumulators of the RIS [SIS] and this example shows that it will be possible to apply the requirements management process to such requirements. Given that no specific ISI requirements have been provided during GDA, I consider this to be an area that should be prioritised by the licensee. This is a shortfall on the scope of the requirements management, and I have captured it under Assessment Finding AF-UKHPR1000-0107.

373. In terms of traceability, the RP stated that the accumulators' requirements will be traced via the item code. As such SDM Chapter 6 (Ref. 98) provides a key link to tie the item codes to the different functions the components support.

374. The traceability of PTR-OFR-24 is described in the RP's requirements management procedure (Ref. 17), but as many of the requirements in this example are not codified, it is not clear how those could be traced without the guidance in the RP's procedure (Ref. 17). This is consistent with what I found in example 5 and it is captured under Assessment Finding AF-UKHPR1000-0108.

Example 8 - High Energy Pipe Failure Requirements and Assumptions for the Fuel Building

375. I chose to sample two High Energy Pipe Failure (HEPF) loadings: IH-HEPF-BFX-02 and IH-HEPF-BFX-07. Each of those internal hazards takes place in different rooms of the BFX hence the different codes.

376. The internal hazards schedule (Ref. 108) refers to the RP's HEPF Safety Assessment Report (SAR) for the BFX (Ref. 109) and identifies the section within this report where the loads are defined. This report is the upstream reference that contains the source of the requirement. The internal hazards schedule also identifies the hazard protection codes, the pipe ID and the barrier ID.

377. The hazard protection codes identify the requirements imposed on the structure by the loading, for example to withstand the loading from a HEPF. In this particular case, those are identified in the DSR and in the 'Reinforced Concrete (RC) Barrier Substantiation Report for BFX' (Ref. 110).

378. The HEPF requirements can be traced backwards and forwards from the internal hazards schedule to the HEPF SAR as both documents contain coding. The traceability to the civil engineering safety case is done through the hazard protection codes, as they provide the link between the internal hazards schedule and the civil engineering schedule, BoSC, DSR and RC barrier substantiation report (Ref. 110).

379. I also sampled the requirements for the combination of hazards, in particular BFX-ICH-01-P01 and the outcome was very similar to the above internal hazards requirements.

380. I consider that for this example the RP has demonstrated an adequate implementation for GDA of its requirements management arrangements.

Example 9 – Aircraft Impact Requirements and Assumptions for the Fuel Building

381. I chose to sample three aircraft impact loadings: EH-AC-BFX-01, EH-AC-BFX-02 and EH-AC-BFX-03. These are external hazards loadings with different probabilities of exceedance.

382. As per the previous example, for EH-AC-BFX-01 the external hazards schedule (Ref. 111) refers to specific sections of two external hazards reports 'Aircraft Safety Evaluation Report' (Ref. 112) and 'Generic Site Related Design Values Report' (Ref. 113) that define the loading. In terms of engineering, the identification of the requirement to protect against the loadings is in the DSR and in the 'Structural Analysis and Design Report for BFX' (Ref. 114). In my opinion, this is consistent with the principle behind SAP ECE.12 regarding the demonstration that the structure can fulfil its safety functional requirements and SAP ECS.3 on codes and standards.

383. In terms of traceability, EH-AC-BFX-01 can be traced backwards and forwards from the 'Aircraft Safety Evaluation Report' (Ref. 112) to the external hazards schedule, but this is no possible with the 'Generic Site Related Design Values' report (Ref. 113) as it does not contain coding, so in this case traceability is one-directional. I have captured the lack of bidirectional traceability under Assessment Finding AF-UKHPR100-0108. As in the previous example, the traceability through the civil engineering reports is done using the hazard protection codes.

384. I also sampled EH-AC-BFX-02 and EH-AC-BFX-03 and the outcome was very similar to the above.

385. I consider that for this example the RP has demonstrated an adequate implementation for GDA of its requirements management arrangements.

Example 10 – Requirements Derived from Temperature and Pressure Challenges to the Spent Fuel Pool

386. The aim of this example was to demonstrate the identification and traceability of requirements from the fault schedule and mechanical engineering schedule to the civil engineering schedule and supporting documents. It should be noted the RP's arrangements identify the flow of requirements from the mechanical engineering schedule to the civil engineering schedule (Figure 2).

387. For this particular example, I considered the expectations from SAPs ECV.2 on defining the safety functions of a containment and SAP ECV.3 on containment requirements. The safety functions for the civil engineering structures are defined at a high level in BoSC, and therefore I consider this broadly aligned with SAP ECV.2.

388. The initial submissions did not contain any requirements that could demonstrate this example, plus the civil engineering schedule was missing all the upstream references (source of the requirement) for the majority of the design basis requirements. I raised this and the RP amended the civil engineering schedule but only for the SFP example and updated the 'Requirements Management Summary Report' (Ref. 16). The updated report (Ref. 16) contained two examples of temperature and pressure challenges, one for the SFP and the other for the BRX.

389. I reviewed the new information provided and I found:

- The requirements can be identified in the upstream reference, but they are not codified.
- Traceability was only possible because the RP provided the route map in the 'Requirements Management Summary Report' (Ref. 16). As the requirements were not codified and the documents did not refer to each other, I could only trace the requirement in one direction, from the civil engineering schedule to the safety analysis document. The same matters (lack of traceability of non-codified specific requirements and one-directional traceability) have been raised in previous examples.
- There was no traceability from the civil engineering documents that contain the requirement, such as the 'Basis of Design for the BFX' (Ref. 106). Again, this is related to the lack of traceability of non-codified specific requirements.

390. My assessment has reinforced some of the matters that I raised in previous examples, but also the need to enhance the links between documents where requirements are transferred. The way to enhance the links will be determined by the licensee, but the current RP's arrangements do not include links between the fault schedule and the civil engineering schedule (see Figure 2), and in my opinion, this is an area that will need to be considered further.

391. This example highlighted that the links between the mechanical engineering schedule and the civil engineering schedule were not developed, and whilst this is understandable as the applicability of the process was limited to few examples, it is an area for further consideration.

392. In summary, for this particular example I judge that the safety case identifies the requirements of the two containment structures sampled (aligned with SAP ECV.3) but the traceability of those through the safety case is not clear. I have captured this shortfall under Assessment Finding AF-UKHPR1000-0108 related to traceability of requirements.

393. Within this example, I found a number of assumptions within one of the analysis documents regarding the modelling and the values taken in the analysis. The assumptions were not codified and given that those were very specific assumptions in a discipline area, I was not able to trace them through the safety case. I have captured the lack of traceability of non-codified specific requirements, such as assumptions, under Assessment Finding AF-UKHPR1000-0107, which covers all the shortfalls related to the scope of requirements management.

Requirements Management - General Findings

394. As mentioned before, the RP provided 'route maps' within the 'Requirements Management Summary Report' (Ref. 16) to assist with understanding the routes through the safety case for all ten examples. It is acknowledged that route maps cannot be provided for every requirement however, each safety case document should contain sufficiently detailed referencing to allow the user to construct a 'map' for each requirement. This is not currently the case, and I consider this a key area for the licensee to address and have captured it under AF-UKHPR1000-0108.

395. In my assessment of the examples, I found inconsistencies between documents, for instance, I found discrepancies between the mechanical engineering schedule (Ref. 96) and SDM Chapter 4 (Ref. 95) regarding the plant items associated with specific safety functions or, as reported in example 1, I found the wrong safety function allocated to a system coding. The licensee will need to review and confirm that safety functions and associated plant items are captured consistently across the design and safety case documentation. I have captured this matter under Assessment Finding AF-UKHPR1000-0110.

Summary of Assessment of Requirements Management Implementation

396. After assessing the above examples, I have summarised below the salient points of my assessment of the RP's approach to identifying and tracing requirements through the safety case:

- The safety case identifies requirements, certainly the most safety significant, and the requirements management process improves the traceability of those requirements. This is aligned with the expectations in SAPs SC.2 and SC.4 in terms of golden thread and SAP EMT.1 regarding the identification of requirements.
- The definition and granularity of the functions and the resulting requirements, as currently presented are not detailed or specific enough.
- The traceability of requirements is largely achieved in the design documents with the requirements management coding helping significantly with this.
- The use of item codes allows the traceability to be further extended into the detailed design and operational documents. While there has been limited specific information available during GDA on tracing requirements through item codes, sufficient has been provided to suggest this could be achieved by a licensee.
- Tracing of the requirements into the safety analysis documentation within the safety case is difficult. The coding (functional or item) is not used in these parts of the safety case, nor is any other means to easily trace requirements.
- The treatment of assumptions does not appear to be consistent with the RP's requirements management process. I have not identified any examples where the RP has treated an assumption as a requirement.
- The traceability of non-codified specific requirements needs further consideration, as the current arrangements are limited and insufficient in some cases.

- Some aspects of the traceability only work in one direction, with the ability to trace a requirement from a lower to a higher level document being the more challenging route.
- The links between the mechanical engineering schedule and the civil engineering schedule have not been implemented. Consideration should be given to provision of links between the fault schedule and the civil engineering schedule.

397. After considering all the above and ONR's expectation on this matter (Ref. 1), I have concluded that, for GDA, the RP has developed adequate arrangements for identifying and tracing requirements through the safety case. I have captured the shortfalls identified in the bullet points above as Assessment Findings.