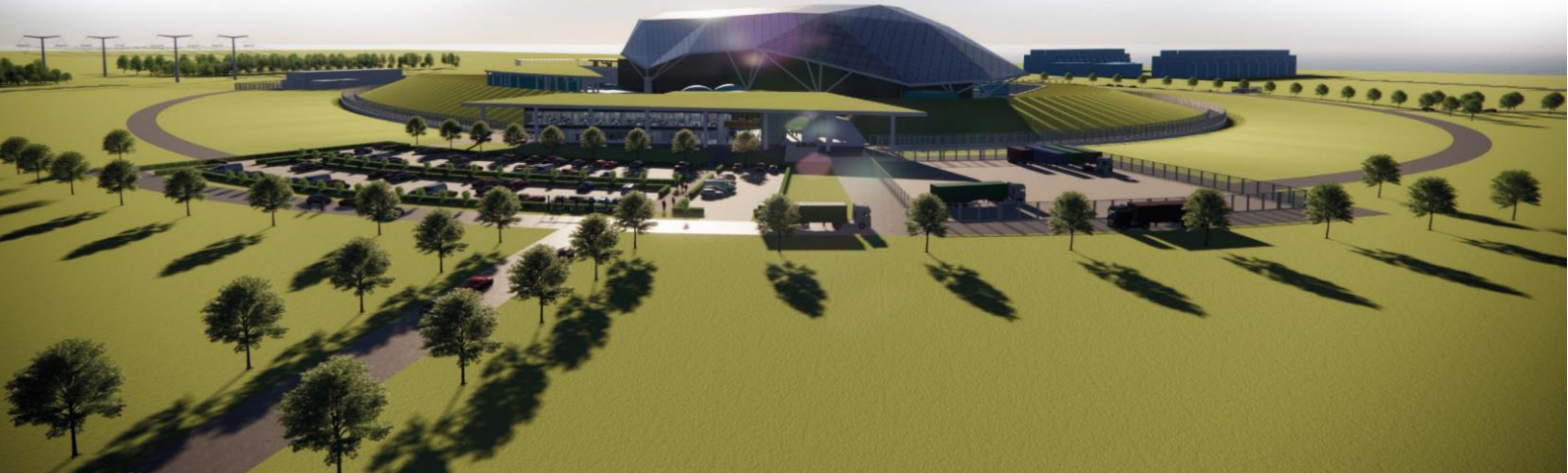
Environment, Safety, Security & Safeguards Case Version 2, Tier 1, Chapter 18: Human Factors Engineering



Record of Change

Date	Revision Number	Status	Reason for Change
March 2023	1	Issue	First issue of E3S Case
February 2024	2	Issue	Incorporates revised approaches defined at Reference Design 7, aligned to Design Reference Point 1, including the refinement of: • Allocation of Function [1]
May 2024	3	Issue	Updated to correct revision history status at Issue 2. Chapter changes include: • Clarification of type of V&V strategies (section 18.3.3) • Additional detail within conclusions section for how arguments and evidence presented meet the generic E3S case objective Also minor template/editorial updates for overall E3S Case consistency.

Executive Summary

Human Factors (HF) applies knowledge of human characteristics to optimise the design of products, equipment, environments, systems and organisations. HF methods are applied to minimise human errors and enhance human performance for a given design. HF methods are most effective when delivered through early engagement with a design project.

The HF assessments aim to demonstrate the high-level claim that 'HF is fully integrated into the Rolls-Royce (RR) Small Modular Reactor (SMR) design and substantiation processes, with the aim of minimising harm to personnel or environment and maximising human performance'. The substantiation of this top-level claim and the supporting sub-claims will develop over the length of the RR SMR programme, as evidence for each becomes available in-line with the design maturity.

This document provides the substantiation of the HF claims, commensurate with the design definition, with evidence provided in a series of supporting documents.

Given the current stage of design development it has not been possible at this time to confirm that all HF claims have been substantiated as greater design definition is required in addition to some areas of testing. However, the analysis of the current concept provides confidence that it will be possible to substantiate the HF claims at an appropriate stage in the design and safety case, as the design continues to mature and as HF guidance continues to be embedded.

HF has been integrated with the design since the commencement of the RR SMR programme design. Multiple forms of guidance have been generated to inform and support the design teams and empower them to incorporate HF guidance independently with the HF Team confirming the application. This allows the HF Team to prioritise their focus on more complex, and higher safety classified components and systems.

The primary assessments to date have been allocation of function (AoF) and task analysis (TA), with limited application of human reliability assessment (HRA), both qualitative and quantitative. These have been, and continue to be, used to assess the design at various stages. They have aimed to optimise the role of the operator, reducing the reliance on the operator and reducing any risks to as low as reasonably practicable (ALARP).

The HRA completed to date has demonstrated there are limited sequences in the probabilistic safety assessment (PSA) to which the operator is a dominant contributor. Whilst the sensitivity studies demonstrate the core damage frequency (CDF) is currently sensitive to the operator contribution to these events, there is still the ability to significantly influence the design including increased automation or remote operation. Additionally, assessing these operator actions in detail, rather than with screening human error probabilities (HEP), is expected to reduce the pessimism within some of these calculations.

There is the continued ability to influence the RR SMR concept as it develops to reduce risks to the operator to ALARP across all lifecycle and operating modes.

Contents

Tables

18.1Introduction to Chapter

18.1.1 Introduction

This chapter of the Rolls-Royce Small Modular Reactor (RR SMR) generic Environment, Safety, Security and Safeguards (E3S) Case presents the overarching summary and entry point to the Human Factors (HF) design and analysis aspects for the RR SMR.

18.1.2 Scope and Maturity

The claims stated in Section 18.1.3 are achieved through the HF programme, which supports the full scope of engineering design and assessment activities across all aspects of the RR SMR power station and factories.

This document content refers to those Structures, Systems and Components (SSC) which are within the Generic Design Assessment (GDA) scope.

At Version 2 of the generic E3S Case, as the design matures towards a final concept definition, the HF integration and assessments continue. The conclusions of this chapter provide a forward look of information still to be developed for this chapter to achieve the generic E3S Case objective.

RR SMR design information presented in this chapter is largely based on the design definition at Reference Design (RD)7 corresponding to design reference point 1 (DRP1) for the generic design assessment (GDA), which is an interim design stage.

Throughout the RD7/DRP1 phase to date, the focus of Human Factors Integration (HFI) has expanded through the following disciplines as the SMR design and E3S Case have matured:

- Design:
    - Update to the Target Audience Description (TAD) [2] and development of the Human Machine Interface (HMI) Style Guide [3] for application to ensure consideration of HF principles and guidance in relation to design
    - Further refinement of the Allocation of Function (AoF) methodology [1] and detailed application across all systems ahead of Design Review (DR) 3 to ensure suitable AoF during system development
    - Extensive task analysis (TA) [4] development based on maturing operating philosophies
    - Support to early development of the main control room (MCR) and associated Control and Instrumentation (C&I) design [5], as a key stakeholder
    - Detailed design support through provision of the HF checklist across the breadth of the SMR design, including manufacture, system and component design, installation and decommissioning
- Environment, Safety, Security, and Safeguards (E3S):
    - Development of a Human Reliability Assessment (HRA) Strategy [6], and application of this through supporting hazard identification (HAZID) activities and identifying and logging human based safety claims (HBSC)
    - HF input to the wider Safety element of the E3S Case through reviewing relevant Operating Experience (OPEX) to support the probabilistic safety assessment (PSA) and

deterministic safety assessment (DSA), both reported in E3S Case Version2, Tier 1, Chapter 15: Safety Analysis [7]

- Early integration with the security team to ensure that HF are engaged in the security aspect of the E3S case at an appropriate time.

Up to RD7/DRP1, the key HF influence on system design has been focussed on systems that have reached RD7/DRP1 maturity. This work will continue as the remaining power plant systems approach RD8. The scope of HF support will then shift focus on to detailed control facility development, substantiation of HBSC and the quantitative aspect of HRA as the safety case develops further.

18.1.3 Claims, Arguments and Evidence Route Map

The overall approach to claims, arguments, evidence (CAE) and the set of fundamental E3S claims to achieve the E3S fundamental objective are described in E3S Case Version 2, Tier 1, Chapter 1: Introduction [8]. The associated top-level chapter claim for E3S Case Version 2, Tier 1, Chapter 18: Human Factors is:

***Claim 18:** Human Factors is fully integrated into the RR SMR design and substantiation processes*

A decomposition of this claim into sub-claims, and mapping to the relevant Tier 2 and Tier 3 information containing the detailed arguments and evidence, is presented in the E3S Case Route Map [9]. Given the evolving nature of the E3S Case alongside the maturing design, the underpinning arguments and evidence may still be developed in future design stages; the trajectory of this information, where possible, is also illustrated in the route map.

A proportionate summary of the arguments and evidence from lower tier information, available at the current design stage, is presented within this chapter. A mapping of the claims to the corresponding sections that summarise the arguments and/or evidence is provided in Appendix A (Section 18.12).

The first level of sub-claims in support of the top-level claim are:

1. HF is integrated into the design based on sound safety principles and methods that minimise risks to ALARP.
2. The RR SMR design provides the operators with the facilities to enable safe and secure operation and reduces risks to ALARP throughout the lifecycle of operation and all operating modes.
3. Human based actions enable safe and secure operation and maintenance of the RR SMR throughout the lifecycle of operation and all operating modes.
4. The RR SMR design is informed by assumptions on the capability of a future licensee from a HF perspective.

This document provides the substantiation of these claims, commensurate with the design definition, with evidence provided in a series of supporting documents. The sections relevant to each claim are:

- Claim 1: Section 18.3
- Claim 2: Sections 18.4 and 18.5
- Claim 3: Sections 18.6, 18.7, and 18.8
- Claim 4: Section 18.9

Section 18.2 provides the Concept of Operations (ConOps) as context to the role of the operator on RR SMR.

18.1.4 Applicable Regulations, Codes and Standards

The Human Factors Integration Plan (HFIP) [10] presents an initial list of standards used to guide and inform the approach to HF for RR SMR. One of the primary standards informing the human factors integration (HFI) programme for the RR SMR design is BS EN ISO 6385: 2016 Ergonomic Principles in the Design of Work Systems [11].

18.2 Concept of Operations

18.2.1 Introduction

A ConOps is a set of information describing the characteristics of a proposed system from the viewpoint of an individual who will use that system. ConOps assumptions relating to RR SMR are discussed in this section. These assumptions will be reviewed as the design matures.

The Power Station Operating Philosophy [12] provides an overview of the systems involved in delivering the power station functions.

18.2.2 Philosophy

The RR SMR is aiming to reduce the need for operators to manually intervene in power station operations, for any lifecycle mode and mode of operation. Whilst automation can be beneficial to reducing the potential for human error or reducing potential harm to personnel, there is a need for personnel to maintain situational awareness.

The AoF process, discussed in Section 18.6, supports the identification of the optimal allocation of activities to person, system, or a combination thereof. The AoF process as deployed for the RR SMR supports the overall aim to reduce claims on the operator.

Therefore, RR SMR concept includes a number of automated and passive safety systems to limit the claims placed on the operator. The interfaces will include features to support the operator in activities assigned to them, whether that is for control or monitoring.

18.2.3 Manufacturing, Construction and Commissioning

Equipment and components for the RR SMR will be manufactured in a number of controlled factory environments. Factory operations are diverse and are expected to include operations such as:

- Fabrication of items
- Construction and assembly of components, systems, modules
- Mechanical handling of equipment
- Machinery operations
- Inspections, including radiography
- Work control systems
- Logistics.

An on-site factory will be available for the construction and assembly of the power station infrastructure, buildings, and systems. This will provide a level of weather protection for the operations and personnel inside the on-site factory.

Manufacturing and construction operations will include automation and remote operations when practicable; however, manual operator actions are still expected for some operations.

The modularised design and the mechanical, electrical and plumbing (MEP) factory will allow for factory acceptance testing (FAT) of agreed SSC within a controlled environment off-site. The remainder of the commissioning (for example: cold and hot functional testing) will take place on site, with the appropriate controls for the activities. Commissioning activities are expected to be largely manual, although the automated systems will be tested.

Factories are outside of the scope of GDA.

18.2.4 Power Operations

Whilst the RR SMR is designed for flexible operations, steady state operation is assumed for the E3S case. It is expected that there will be only minimal requirement for manual adjustment of reactivity, e.g., to manage fuel burnup. The turbine systems will respond automatically to small changes in grid frequency.

Fundamentally, the reactor is expected to operate in two distinct modes; power operations, and shutdown operations to permit outages and refuelling periods. These can be divided into six modes of operation, which are largely similar to the modes of operation for existing pressurised water reactor (PWR):

1. Power operations
2. Low power
3. Hot standby
4. Hot shutdown
5. Cold shutdown
6. Refuelling.

Fourteen control facilities have been identified to support the through-life operation of the RR SMR. These include facilities which provide support to on-line operation, such as the MCR, security control centre (SyCC), and radioactive waste control room (RWCR). Other facilities support offline operation such as the outage control centre (OCC), with additional facilities to support emergency preparedness and response, such as the emergency response centre (ERC). Section 18.5 provides further discussion.

During power operations, monitoring and control of the RR SMR will be centralised within the MCR, located within reactor island (RI). From here, the operators monitor and control the reactor response to changes in turbine load, driven by demand from the facility which the RR SMR is supporting, e.g., the electricity grid. The current MCR concept allows it to be staffed by two operators with a single supervisor, with space for additional personnel to support, e.g., during a transient. The bottom-up staffing assessment will confirm the appropriate requirements for RR SMR.

A detailed list of the operating limits and conditions (OLCs) will be developed for the design to provide the operators with boundaries of operation. These will include parameters such as temperatures, pressures, status of SSC and activity limits, the required acceptance criteria, for example, limits, and will be detailed in technical specifications.

From the MCR, the operators are able to take action to correct identified deviations; however, the passive nature of the plant means that no remote operator actions are required within the first 30 minutes of a fault occurring. Passive systems provide the initial protection against the faults identified as design basis initiating events, which challenge control of the key functions that maintain reactor safety.

In the event that the MCR is uninhabitable, e.g., due to fire, then the operators will transfer to the supplementary control room (SCR). The SCR is also located within RI, located such that a single incident shouldn't threaten both control rooms but also to allow safe transfer of personnel within

the appropriate time. The SCR will include monitoring and control of safety systems, in order to ensure a safe state is achieved and maintained.

Whilst the power station is operating, the personnel across the power station will be conducting examination, maintenance, inspection and testing (EMIT), and recording and/or reviewing the results of analysis, e.g., sampling of coolant, which confirms the power station is operating within normal operating bands. These activities are expected to include both manual and automated actions.

During power operations it is anticipated that personnel will also be planning for the next outage period, undertaking training, and meeting with regulators as part of normal duties amongst other activities.

Some aspects of fuel handling will take place during power operations; preparing for refuel operations, monitoring and managing spent fuel within the spent fuel pool and at the spent fuel store, and moving spent fuel to interim storage. These activities are anticipated to include both manual and automated actions, noting that many of the manual actions would be remote given conventional and radiological risk.

RR SMR will provide amenities such as food outlets, changing facilities, toilets, showers, and storage locations for personal items on the site.

It is expected that some level of training facility will be provided on-site, but the option is available for a full-scope training facility to be provided off-site. Similarly, an element of business control is expected on site, but the location of full business, finance, planning, human resources capabilities etc, could be off-site.

18.2.5 Outage and Maintenance

Outage operations will include activities such as mechanical handling of plant equipment, crane operations, fuel handling, use of specialised tooling, management of fuel pools, and invasive maintenance activities.

These activities are anticipated to require more operator actions than normal critical operations although an appropriate level of automation and remote operations will reduce the need for direct operator intervention.

Fuel handling will be required to refresh the fuel in the reactor core, and to remove spent fuel into an approved container (flask). Flask handling and preparation for storage will be conducted on-site, in addition to monitoring of the stored fuel. These activities will be conducted and controlled locally, via remote controls where possible. The ultimate fuel and waste disposal facility will be located off-site.

18.2.6 Decommissioning

Decommissioning activities are being considered in the design of the facility and site. decommissioning activities will be required to remove materials and infrastructure from the facility / site such that the site can be re-used. Decommissioning will include the handling and storage of radioactive materials and waste, removal and disposal of systems and equipment, de-construction and demolition of facilities and buildings, and restoration of the site to a usable condition.

Many of these activities will be unique to the decommissioning phase of the lifecycle and are anticipated to include many local actions. E3S Case Version 2, Tier 1, Chapter 21: Decommissioning and End Of Life Aspects [13] discusses decommissioning in further detail.

18.2.7 Staffing

The RR SMR aims to have a reduced number of personnel compared with traditional large nuclear stations. This will be realised through increased automation and remote operations where safe and practicable to implement. In addition, the fleet support approach allows for some operations to be shared across stations, e.g., stores or outage planning, which reduces the number of personnel per site.

The on-site personnel numbers will need to remain sufficient to provide the required operations across all lifecycle modes, and against normal, faulted, and post-accident scenarios.

A 'top-down' staffing concept [14] has been generated using available operational experience. The primary purpose of this is to provide an initial view of the number of personnel required on-site, which need to be accommodated within the design. It also provides a basis for assumptions on the staff available to support activities.

This concept currently considers the power operations phase of the lifecycle; additional staff would be required to support outages.

This iteration of the staffing concept results in the following:

- 318.5 full time equivalents (FTE) aligned to a single RR SMR
- During the day, e.g., 9am – 5pm, 191.5 FTE are required to support and deliver the functions of the RR SMR. The remaining staff are shift workers who are on their rest days. Of these 191.5 FTE, it is estimated that:
    - 98.5 FTE are required to be based on-site
    - The remaining 93 FTE deliver functions which could be based off-site, dependent on the future owner/operator's arrangements. If required, these FTE can be accommodated on-site. The site layout will provide space for personnel based off-site to visit the RR SMR as required, e.g., meeting rooms, flexible working spaces.

In the subsequent design phases the TA, and substantiation of the HBSC and human based security claims (HBSyC) will inform a bottom-up assessment of the staffing levels required in support of the claims made in the E3S case.

The TAD [2] (Section 18.4) details the anticipated characteristics of the future operator.

18.3 Human Factors Integration

18.3.1 Introduction

This section provides substantiation of the following hierarchy of claims:

1. 18.1.1 HF are integrated into the design based on sound safety principles and methods that minimise risks to be ALARP.

1.1 18.1.1.1 A suite of HF activities have been carried out to integrate HF into the RR SMR design.

1.2 18.1.1.2 HF requirements have been derived from principles, standards, relevant good practice (RGP) and OPEX.

HFI is the process by which the people component is considered throughout the design lifecycle of a product. It is a systematic process for identifying, tracking, and resolving human-related considerations to enable the balanced development of both the technology and the human aspects of design.

HF has been integrated with design from the beginning of the RR SMR project and been an integral part of the RR SMR programme since its inception, providing early support to key design decisions.

Within the earlier design phases this early integration was continually delivered through publication and communication of the HFIP [10], and consultation for design and decision reviews. HF guidance was produced and shared across the design areas to provide awareness, and design requirements.

Through the previous design phase this integration was formalised through the creation of verifiable requirements which are allocated to the relevant design areas through RR SMR requirements management system. This systematic approach to requirements ensures visibility of the requirements to all relevant areas as well as a simple mechanism for the tracking of compliance with the allocated requirements.

At each SSC definition review (DR) stage, compliance with these requirements is evaluated with any non-compliance requiring evidence of their progress towards compliance. Details on how the requirements are evidenced and substantiated is discussed in Section 18.3.3. This evaluation of the achievement of HF requirements is provided by HF suitably qualified and experienced personnel (SQEP).

Each SSC is required to populate a HF checklist which is reviewed by HF SQEP. The HF checklist provides a means of understanding each SSC and the anticipated interaction with personnel through the lifecycle of the SSC. It also directs the SSC owner to relevant HF guidance and standards that they will be expected to embed within their concept to ensure successful HFI.

Integration of HF support into the key design decisions is achieved by ongoing dialogue with the design teams from hazard identification (HAZID) input and flow-down of HF requirements. This is supported through population of a HF checklist as part of the systems DR process, and provision of associated design support as required.

The HF Risks, Assumptions, Issues, Dependencies and Opportunities (RAIDO) register [10] captures any identified risks and issues, including non-compliance with HF requirements even if these non-compliances can be accepted.

Leading up to RD7/DRP1, HF support has focused on supporting early system definition, design decisions, and identifying the key safety related operator actions, predominantly through:

- Design:
  - To ensure consideration of HF principles and guidance in relation to design
  - To ensure suitable AoF during system development [1]
  - To support early development of the MCR and associated C&I design, as a key stakeholder, summarised in [5]
- Environment, Safety, Security, and Safeguards (E3S):
  - Safety – HF input to the safety element of the E3S Case
  - Security – early integration with the security team to ensure that HF are engaged in the Security aspect of the E3S case at an appropriate time.

18.3.2 Human Factors Integration Plan

The way in which HFI is planned and managed to support successful achievement of the HF objectives is defined within the HFIP [10]. The HFIP is also used to ensure a consistent and robust approach to the application of HF principles across the project and is updated as necessary to address the developing design solution at key design stages.

The HFIP [10], is the coordinating document for all HFI activities in the project, defining how the HF activities necessary for successful delivery of the design will be conducted, detailing the:

- Scope of HFI activities
- HF organisation, programme and resource
- HFI strategy
- HF standards
- HF methods.

HFI across the SMR project has developed, and will continue to evolve, in line with the structured development of the integrated design and E3S case. This has been supported by the project being instigated on the basis of a systems engineering approach to design, which is requirements led. Requirements for the RR SMR are defined in the RR SMR requirements management system, with a copy of the current requirements document in [15]. HF activities are therefore performed with progressive detail to support design decisions and provide evidence that the design supports safe, effective, and efficient operation by the target users.

The strategy for HFI into the RR SMR design is based on early engagement with the design teams, supported by early delivery of design policies and guidance. Recognised HF methods are being applied to the identification and analysis of human-system interactions commensurate with the design maturity, requirements of the E3S case, and the lifecycle stage, with iterative development across activities as required, and will continue as the design develops and matures through to developed design (DD).

Each of the methods are discussed within the HFIP [10], and will be applied as appropriate to the design phase and topic. As the RR SMR design progresses through the lifecycle, HF activities will be performed with progressive detail to support design decisions and provide evidence of the design against human actions important to safety.

For the RD7/DRP1 phase, HF support to design has built upon the TA of human-system interactions developed in previous phases, to support early system definition and the design decisions. The TA [4] and AoF assessments [1] extend across the RR SMR, to provide a more detailed assessment. This has optimised the balance of tasks between human and engineered systems and minimised the dependence on human-based actions to support delivery of safety measures.

During RD7/DRP1, a structured approach has also been developed for integrating HF into manufacturing and security. Support to manufacturing and security have not progressed significantly during the RD7/DRP1 phase.

18.3.3 Requirements

There are two HF related requirements recorded at 'Level 0' for the Power Station in the RR SMR requirements management system for the RR SMR:

1. The SMR shall ensure that risks to all populations from conventional safety hazards during all modes of operation and lifecycle stages are reduced to levels that are ALARP.
2. The SMR shall be capable of safe operation by personnel with the characteristics of the TAD [2].

These requirements are decomposed further through the transverse module, and then allocated to the relevant teams across the SMR programme, e.g., layout and installations, components, etc. This systematic approach to requirements ensures visibility of the requirements to all relevant areas as well as a simple mechanism for the tracking of compliance with the allocated requirements.

As these requirements are applicable to a large range of SSC, they do not provide a specific requirement such as 'provide a space envelope of x metre' as these are context specific but instead signpost the user to relevant documents, such as the TAD [2], for the specific data they require. Topics covered in the requirements include physical space, temperature, lighting, and adherence to the HMI Style Guide [3].

The achievement of these requirements is monitored through the design maturity review gates, with HF having the ownership of agreeing the requirement status for each SSC the requirement is allocated to.

HF is a key representative at DR. During the DR, compliance with the allocated requirements is evaluated as appropriate for the design phase with any noncompliance requiring evidence of their progress towards compliance. This evaluation of the achievement of HF requirements is provided by HF SQEP.

The DR Checklist (within RR SMR Limited requirements management system) includes an additional prompt for the appropriate HF assessments to have been completed for the stage of the programme, which also requires confirmation from HF SQEP. Both of these directly inform the conclusion of the DR.

HF are also a stakeholder in decision reviews, with HF a topic for designers to explicitly consider within the Detailed Evaluation of Options within the Decision Record. Additionally, HF are a key stakeholder for HAZID and Hazard and Operability (HAZOP) study, discussed further within Section 18.7.2.

18.3.3.1.1 Compliance with Requirements

Verification and validation of HF requirements within the associated SSCs to demonstrate compliance, will be undertaken inline with SMR0008444 Rolls-Royce SMR Approach to Verification and Validation [16]. These strategies are in various stages of maturity across the plant but may be

based on analogy, analysis, or testing with the activities being undertaken by the designers, in conjunction with HF or by HF, depending on the nature and/or complexity of the requirement.

To ensure that guidance and HF standards are being used consistently across the RR SMR design, Verification and Validation (V&V) assessments will be carried out once the design has progressed. The V&V can be carried out through multiple methods including anthropometric assessments, Virtual Reality (VR) as well as the control room simulator.

These methods will be able to provide accurate representation of the current plant and will be able to demonstrate any issues within the design including any access, HMI design etc.

18.3.4 Guidance

A series of HF policy documents were initially developed to provide policy statements, guidance, and a preliminary identification of codes and standards suitable for application to the RR SMR project in support of achieving the formal HF requirements:

- Accommodation of Humans into the Built Environment [17]
- Minimising Human Error [18]
- Staffing, Job Design and Training [19].

The guidance provided within the policies aims to provide the design teams with an understanding of how the policies and requirements should be implemented and achieved. The guidance is supported by references to the relevant codes and standards if further information is required.

HF awareness training is also provided to supplement any guidance provided.

For some topics the provision of guidance allows for a graded approach to HFI, with designers making use of other supporting guidance for simple interactions. Subsequently, more detailed design guidance documents, such as the TAD [2] and HMI Style Guide [3], have been produced drawing upon specialist support for more complex examples to aid designers in implementing good HF design practice and further support meeting requirements.

For example, a graded approach which increases the involvement of HF specialists and analysis based on the complexity of designing and demonstrating accessibility has been developed as follows:

1. The designer includes a ‘space reservation’, or ‘space envelope’, for accessibility in their design. Dimensions for access, reach and clearance for different postures are provided in the TAD [2]. Evidence of accessibility is provided by meeting the relevant space reservation from the TAD [2].
2. The designer draws upon detailed accessibility data in a relevant standard. Support to the designer in the selection of relevant standards and data will be provided by the HF resource. Evidence of accessibility is provided by reference to the relevant standard and a record of application of the standard in the design.
3. The designer identifies an accessibility scenario that is not addressed by simple space reservation or data from the available standards. The designer works with the HF resource to agree a design solution to optimise accessibility. Evidence of accessibility is provided by analysis by the HF resource.
4. The designer identifies a complex accessibility scenario with multiple constraints. The designer works with the HF resource to agree a design solution to optimise accessibility, including the

option for virtual or physical mock-up of the scenario to assess accessibility. Evidence of accessibility is provided by detailed analysis by the HF resource.

HF specialists support the design teams in their application of the guidance, and complete specific analysis as required to provide the appropriate verification evidence. One method of sharing the guidance in the policies in a targeted way is the HF checklist. The HF checklist supplements this guidance, by identifying key aspects which the designers should consider.

Finally, to support HRA, two strategy documents were developed to provide guidance for development of HRA to support the E3S case in achieving the formal HF requirements:

- Human Reliability Analysis Strategy [6]
- Human Reliability Analysis: Quantitative Assessment Strategy [20].

These documents detail the approach and qualitative and quantitative methods to identify and assess the contribution people make to risk, demonstrate that actions can be discharged effectively and reliably, and substantiate the role of the operator within a complex system.

18.3.5 HF Checklist

The purpose of the HF checklist is to provide each SSC designer with a structured overview of what a HF SQEP would expect to see in the SSC design. It also equips the designer with information required to integrate HF into their design from the start of the design process at DR0. By populating the HF checklists and using the documents and standards provided, they are working towards the HF requirements against them in the RR SMR requirements management system.

The HF checklist allows the SSC owner to independently initiate the application of HF guidance and standards to aspects of their concept, such as the physical integration of humans. This allows the HF SQEP to prioritise their initial support and assessment on areas of greater complexity, or areas finding the HF requirements challenging to fully achieve. The SSC designers can engage with HF SQEP during production of the HF checklist and is required to engage further following initial population.

Where operator interaction has been identified, the HF requirements, policy documents, and guidance documents are being used to inform the design to ensure it is suitable for use. The HF checklist supplements this guidance by identifying key aspects which the designers should consider and is a live support tool which enables tracking of compliance with HF guidance by the designers.

The outputs of the HF checklist include:

1. Title Sheet:
   a. Captures information regarding the SSC as well as a record of HF checklist document change to enable accurate tracking of each HF checklist throughout its design.

2. Initial Question Set:
   a. Presents key HF topics such as Controls and Displays, Alarms and Workspace Design, covered by the HF checklist with a single yes or no question. The SSC designer is to answer each of these questions in relation to the SSC captured in the title sheet.

   b. Answering ‘yes’ to a question indicates that the HF topic presented in the question is relevant to the design of the SSC, whereas answering ‘no’ means the HF topic is not involved/relevant to the SSC.

3. Required Checklists

a. Once the SSC designer has identified which HF topics are relevant to their SSC by answering the initial question set, a more comprehensive set of questions for each of the HF topics that were answered 'yes' to is presented.

b. Each topic typically consists of seven questions (yes or no answers) with space to document evidence or justification for the answers given. It is expected that as the design matures, all the questions should be answered and evidence (to support a 'yes' answer) or a justification (to support a 'no' answer) provided in the space allowed next to the answer.

4. HF Data Tables

a. Primary and secondary information has been provided for each relevant question. Primary information constitutes RR SMR HF documents and policies which provide the information required. Secondary information constitutes relevant standards and best practice guidance.

b. Each HF topic in the checklist has also been associated with the transverse requirements that they are relevant to. This way, SSC designers can ensure that by answering the HF checklists and using the documents and standards provided they are meeting the HF requirements against them in RR SMR requirements management system.

Implementation of the HF checklist is monitored by the HF team. Completing an initial version of the HF checklist is a required output for DR3; an SSC will not pass this design gate without engaging with the HF checklist process.

At RD7/DRP1, 83 HF checklists have been created and reviewed. Of the 83 HF checklists, 37 have attended one or more drop-in session to review the checklist progression. The majority of the HF checklists have been for systems within the RI, however they have also been developed for other areas within the plant.

Continued design support through the application of the HF checklist and detailed design guidance is an on-going iterative process to ensure that good practice HF is incorporated into the design at an appropriate time.

18.3.6 Risks, Assumptions, Issues, Dependencies and Opportunities Register

HF issues are identified, tracked, and managed to resolution via a RAIDO register [10]. Issues may arise where HF requirements conflict with engineering requirements or constraints, e.g., access requirements are not met as a result of equipment being positioned to deliver an engineering function, such as vent valves being located high in the system.

The RAIDO will be managed by HF resource, with significant HF risks or issues reflected within centralised registers for the SMR project. This approach allows HF issues to be considered alongside engineering issues and supports identification of balanced technical solutions to issues.

No significant risks or issues have been logged within the RD7/DRP1 phase. As is to be expected for a maturing design at RD7/DRP1, the design concept continues to change and develop and therefore whilst the concept may not be optimal in all areas there is still opportunity to influence and change the design.

18.3.7 Conclusions

There is clear evidence of HFI across the RR SMR programme, supporting the claims identified in Section 18.3.1. The approach to HFI empowers design teams to initiate less complex assessments, for

example placing manikins within the Computer Aided Design (CAD) model to evaluate the achievement of physical space requirements. This allows the HF engineers to focus on the more complex areas of the concept and the application of specialist techniques.

The role of the HF team across Definition, and Decision Reviews, HAZID, HAZOP, and design development meetings, demonstrates the integration of HF into all aspects of the design. HF have not identified any significant risks however, as the RR SMR concept continues to develop through the subsequent design phases, HFI will continue to be necessary.

18.4 Target Audience Description

18.4.1 Introduction

This section provides substantiation of the following hierarchy of claims:

1. 18.1.2 The RR SMR design provides the operators with the facilities to enable safe and secure operation and reduces risks to ALARP throughout the lifecycle of operation and all operating modes.

2. 18.1.2.1 The RR SMR design accommodates the target population.

3. 18.1.2.1.1 A suitable RR SMR target population is defined.

4. 18.1.2.1.2 The RR SMR target population is accommodated in the design.

18.4.2 Target Audience Description

Purpose

The TAD [2] is a guidance document developed by HF to define the physical and cognitive characteristics of a defined target user population who will support the manufacture, build, operation, maintenance, and decommissioning of the SMR.

Based on these characteristics, the TAD also contains specific design guidance to help ensure the SMR facility, systems and equipment adequately accommodates the full range of target users.

To accommodate the physical characteristics of the TAD the design limitations are based on a higher upper percentile of a United Kingdom (UK) population of 1st - 99th percentile. This will both accommodate secular trends and the wider global population given the global ambitions of RR SMR. The information presented in the TAD is organised according to the following structure:

1. Physical characteristics: considers the anthropometric characteristics of the operators, e.g., body size, strength; from which, design requirements can be developed (e.g., clearances and access for ingress/egress, location of controls).

2. Physiological capabilities: considers aspects relating to thermal, tactile, visual, and auditory capabilities of the operators, e.g., field of view, line of sight.

3. Psychological capabilities: outlines the capabilities of the operators relating to aspects such as cognitive perception and processing, memory, workload, and situational awareness.

4. Skills and knowledge: outlines the background and experience, training needs, skills and knowledge of the operators.

The fundamental physical, physiological and psychological characteristics described in the TAD will apply to all user populations. However, adjustments may be required to physical dimensions for clearance, reach and access to account for tooling/equipment and any special clothing or Personal Protective Equipment (PPE) requirements specific to any user population.

The information and data provided in the TAD describe the current user populations, with discussion provided on the impact of secular change for physical characteristics. Where practicable, additional

margin will be included in the associated design requirements to provide a robust solution with the capacity to cope with future population changes.

A non-compliance process has been developed during RD7/DRP1, to ensure consistency across the RR SMR when deviating from documented guidance. The non-compliance process uses a flowchart to resolve the issue of concern in a consistent manner that records any mitigating rationale for any non-compliance approval.

At each key step, the route to resolution is provided, ranging from local agreement for a minor non-compliance through to escalation to the Chief Plant Engineer.

A log demonstrates how non-compliances are managed, providing a record to demonstrate that process is being used consistently whilst still maintaining an ALARP design. If the non-compliance is significant and there is no immediate resolution, it will be recorded in the RAIDO for further consideration or potential escalation.

The non-compliance process helps to ensure that the outcome is still ALARP.

An example of an accepted non-compliance is the potential need to 'duck' underneath pipework on occasion given the height of the modules and complexity of pipework routing. HF assessed the request and have produced and issued a supplementary document, [21], providing guidance on when it is acceptable to require operators to 'duck' underneath pipework, ducting etc which traverses a walkway.

The 'ducking guidance', [21], has been issued to the layout/installations team to give specific guidance on these scenarios, such as the acceptable depth of protrusion into the height of the walkway, the acceptable width of the protrusion, and the acceptable distance of a protrusion from a doorway. HF continue to aim to remove the need for operators to duck; however, the height of the modules means this may be required occasionally.

Application

The TAD [2] applies to all areas of RR SMR and is referred to from the requirements within the RR SMR requirements management system. This ensures that the TAD requirements are formally integrated within the SMR design.

During RD7/DRP1, the TAD has been used in support of the development of design and plant layout to inform, confirm and check dimensions. Physical module reviews have also been carried out by HF. The purpose of these reviews is to ensure early engagement with HF and compliance to the TAD [2]. As more detail is added to the physical module demonstrators, further HF reviews will be undertaken.

At RD7/DRP1, few compliance issues have been identified, but where the design is unable to meet the requirements within the TAD for example, commercial off the shelf (COTS) equipment, the formal non-compliance process is followed. This ensures consistency when deviating from the TAD whilst still ensuring that the risk is ALARP.

A VR facility has been established and used to evaluate more complex aspects of the layout concept, for example access above C&I cubicles for the installation and inspection of cables. It is anticipated that this facility will be used extensively in the forthcoming design phases as further detail is included in the layout concept.

The design teams are able to select the appropriate data from the TAD [2] to use, however the HF team will evaluate their use of the data and if required provide them with the correct data set to use.

18.4.3 Conclusions

The TAD [2] is linked from the requirements in RR SMR requirements management system, which are allocated to teams to formally provide evidence against at the design maturity gates. This ensures that the TAD requirements are integrated within the SMR design.

The non-compliance process has been used to reach appropriate compromises with the design teams. These non-compliances have been minor, for example allowing 95th percentile measurements rather than 99th percentile measurements, therefore the non-compliances have been sentenced within the HF Team.

It is anticipated that the 3D and VR tools will be used significantly when evaluating the layout concepts in further detail.

18.5 Human Machine Interface Development

18.5.1 Introduction

This section provides substantiation of the following hierarchy of claims:

1. 18.1.2 The RR SMR design provides the operators with the facilities to enable safe and secure operation and reduces risks to ALARP throughout the lifecycle of operation and all operating modes.

2. 18.1.2.2 The RR SMR equipment and layout supports the reliable performance of the operators through-life.

3. 18.1.2.2.1 Controls and indications are provided for the operator.

4. 18.1.2.2.2 The layout of RR SMR enables safe and reliable performance of the operator through-life and through all operating modes.

Interfaces must support the operating personnel in the delivery of their role in power station operations. Interfaces will be designed to provide suitable and sufficient user interfaces at appropriate locations to provide effective monitoring and control of the facility in normal operations, faults and accident conditions.

The RR SMR design at RD7/DRP1 identifies 14 control facilities from where the operators will interact with the power station using a variety of HMI. The report [5] defines the purpose of each existing control room. Topics considered for each of the control facilities include functions; location & size; welfare provisions; habitability; communications; personnel; equipment; control panels; and room layout.

Examples of these locations include:

- MCR
- SCR
- SyCC
- ERC, on-site, with ERC off-site
- Local interfaces.

In addition to fixed locations, it is anticipated that operators could have mobile devices which could record maintenance activities or provide operating instructions, plant data etc.

During RD7/DRP1, HMI development was related to the larger, fixed control locations rather than local or mobile interfaces. These local interfaces will be incorporated into the concept through the subsequent phases as the required controls and indications are identified and as the layout concept is matured.

18.5.2 Design Development

Operations

The MCR will be the primary location for controlling and monitoring RR SMR. The SCR will be used in the event that the MCR becomes inoperable and/or uninhabitable during operations, e.g., due to an internal hazard such as fire.

The ERC will co-ordinate the activities required to manage the response to events such as fires, security incidents or release of radiation. In the event that the ERC cannot manage the event, or requires wider communication with neighbouring communities or institutions, then the off-site ERC would provide support or take control of the event as required. The site layout and staffing concepts will ensure that the required emergency arrangements are achievable; this is described further in E3S Case Version 2, Tier 1, Chapter 19: Emergency Preparedness and Response [22].

The Technical Support Centre (TSC) will provide technical assistance to the MCR or SCR, via the ERC, in the event of a reactor incident/accident/fault.

The Operational Support Centre (OSC) will provide space to prepare emergency responders for their duties. The OSC shall form part of the ERC. The primary function of the OSC is to provide space for responding personnel to gather, receive briefings and get equipped for the duties they are to perform in response to the emergency.

Location

At RD7/DRP1, the MCR is located within the RI and TI security boundary to protect against unauthorised entry. The MCR will be located within the hazard shield, and on the aseismic bearing, with welfare and habitability provisions to ensure operability and habitability during normal operations and accident conditions. The SCR shall be located outside of the hazard shield, such that internal hazards cannot simultaneously affect the MCR and the SCR. This concept provides protection against external hazards for the personnel based within the MCR, whilst providing sufficient segregation between the MCR and SCR in the event that the MCR requires evacuation.

The ERC, TSC, and OSC shall be co-located together, either directly adjacent to the other or connected by a short corridor and have access to separate adjacent rooms for teams performing independent tasks. This allows the ERC to maintain overall control of the emergency response whilst also having direct access to other supporting functions of the ERC.

The ERC shall be located outside of RI in the administration block.

Size

The RR SMR Control Rooms Outline Description, [23], provided an initial view of the control room solution for RR SMR, based upon a review of industry standards and relevant good practice.

Reference [23] provided sizing estimates for the MCR and SCR. These size estimates were based on existing large nuclear power stations which were considered reasonable at RD7/DRP1 as the control room size is less dependent on the power output of the power station than it is on the interface design, e.g., personnel levels, the extent of hardwired controls and indications compared with software based, and the diversity or redundancy required in the systems supporting the control room displays. It is anticipated that the expanded use of screens will reduce the volume of space required, however the space envelope has been retained at this stage to manage the level of uncertainty with the control room content.

Interface

The classification of the systems being controlled or monitored influences the required classification of the control systems and the technology which can be used in the control room.

Within the RD7/DRP1 phase, C&I, HF, Safety and Systems Teams progressed the identification of functions which require control and/or indication within the control rooms. The need for control and/or indication has been identified through various mechanisms, including reviews of operational experience, the RR SMR Fault Schedule, TA, and AoF.

The functions already identified as requiring control and/or indication require a combination of hardwired and software-based interfaces. The selection of hardwired compared with software-based interfaces will consider the safety classification of the function to be interacted with.

The key principles for designing control interface have been defined and provide guidance on key areas of HMI design to facilitate the creation of clear, concise, and consistent HMI control designs to minimise the chance of human error occurring whilst interacting with controls [3]. The HMI Style Guide, [3], ensures consistency across the RR SMR power station design. As the design develops, the HF team will work with the relevant teams to ensure that the HMI Style Guide [3] is being considered and used.

At RD7/DRP1, HMI have not been developed for the RR SMR control facilities; however, key architecture features have been identified which would be required of the C&I, e.g., synchronous alarm flashing.

The identification of the functions which require controls and/or indications will continue through into the subsequent design phases.

Verification and Validation

CAD and VR are currently available to verify that requirements for the provision of adequate space have been achieved, and to support the definition of interfaces.

A MCR demonstrator is currently being procured and developed to support V&V. This demonstrator will be used to test, review, and iterate the MCR design, and support HMI design by using TA to create a list of the C&I required.

It is recognised that a full scope, high fidelity simulator is a valuable tool for both developing the design of the control room and HMI, and for confirming that requirements have been achieved.

The definition of the simulator requirements and programme is continuing.

The subsequent design phase will include trials to develop the physical size and layout of the control rooms, with some paper or screen-based representations of HMI to test potential HMI concepts.

Subsequent phases will include evaluations of procedures, and operator workload.

18.5.3 Conclusions

The identification of operator actions is continuing, and therefore the required controls and indications have not all been identified. Using Operational Experience, Space Claims for the control facilities have been secured within the concepts to ensure the RR SMR design provides for the required control facilities.

Throughout the subsequent design phases the equipment required within these facilities to support the claims will be identified and sized. In addition, the equipment and space required for local control stations will also be identified in the future design phases.

As discussed in Section 18.4 the TAD is, and will continue to be, used by the layout design teams to include the required provisions for the operators.

18.6 Allocation of Function

18.6.1 Introduction

This section provides substantiation of the following hierarchy of claims:

1. 18.1.3. Human based actions enable safe and secure operation and maintenance of the RR SMR throughout the lifecycle of operation and all operating modes.

2. 18.1.3.1 The operator actions required to operate and maintain the RR SMR are identified.

3. 18.1.3.1.1 Processes and actions are appropriately allocated between machine and operator.

These claims are supported by the HF AoF activity which aims to assign those functions required to meet system goals to an optimised combination of human and engineered elements of the design. This activity is led by HF and is supporting the aim to reduce operator burden with the majority of functions being allocated as fully automated.

As a result, tasks for which humans are known to have reduced levels of reliability, such as long-term monitoring, are assigned to the engineered elements of the system, thereby reducing the potential for human error. Conversely, tasks at which humans show improved performance, such as complex decision-making, are not automated in order to improve overall system performance.

The approach to AoF for this phase is presented in [1] and describes the AoF methodology and its application in support of the development of RD 7, including the provision of design guidance such as interface requirements.

Consideration of AoF must be made during optioneering and throughout the continued development of the plant design and E3S case and align with the overall RR SMR design philosophy and E3S case claims and assumptions.

AoF is applicable to all design functions, including both safety and non-safety related. The AoF method described in [1] supports the implementation of any AoF decision, including detailed design of any engineering support to the human elements of function delivery.

AoF is an iterative process and, as the design develops, AoF will be revisited to ensure the appropriate Level of Automation (LoA) has been applied.

18.6.2 Methodology

A simple allocation between either fully manual or fully automatic is not expected to produce a design where overall system performance is optimised. Therefore, the AoF between human and engineered elements of a system requires consideration of increasing levels of automation.

At RD6, the RR SMR AoF process was based upon an Electrical Power Research Institute (EPRI) methodology, that uses a description of increasing LoA (Levels 1-10) based on a scheme proposed by Endsley [24] and arrived at through the use of a flowchart to guide the analyst through a series of questions to identify the optimal level of automation. These questions were standardised and provided consistency to the analysis. The questions provided a prompt to the analyst to consider topics including if the function is central to the human role, if the function is essential in providing situational awareness, or if the function challenges human capabilities.

This was supplemented by:

- Development of a functional characterisation (FC) assessment to assist in determining whether the function may be more suited to automation or manual operation.
- Structured consideration of Endsley's 10 LoA, [24], to support development of more specific design advice when the output recommendation was for 'partial automation'.

For RD7/DRP1, the AoF method applied to the RR SMR design is updated to consider the lessons learned from the application of the earlier method, and an update to the EPRI guidance on AoF as detailed in the Human Factors Analysis Methodology for Digital Systems, [25].

This guidance document provides more detail on the function definition and analysis. The revised process includes consideration of additional aspects including impacts of failure and the need for adaptive allocation rule, and points for consideration in defining shared allocation. The guidance also provides further function allocation decision criteria covering mandatory and informed allocation, human capability and assessing both technical and economic feasibility of automation.

It is noted that the AoF assessment method will be subject to review and iteration as the design solution matures, or for new or modified functions.

18.6.3 Analysis

The scope of AoF analysis performed during RD7/DRP1 has focussed on safety critical systems that are within GDA Step 2 scope, with the assessments being undertaken against the functional requirements placed on those systems.

Systems have been prioritised for assessment based on the level of maturity and progression towards DR3 as presented in Design Maturity Timeline, [26]. Completion of an initial AoF is a requirement in passing DR3; therefore, systems due to progress through DR3 sooner were prioritised.

In total, 234 functions across 28 systems have been analysed in support of RD7/DRP1, with design advice provided to system owners for incorporation to the associated system design description (SDD) / safety measure design description (SMDD). Provisional system design proposed by system owners predominantly aligns with the AoF output from the analysis.

In line with the key design principle of the RR SMR, the trend to automate remains dominant with approximately 62 % of the assessed functions being fully automated.

In contrast, approximately 9 % of the assessed functions are allocated to manual (local or remote) tasks.

Finally, approximately 29 % of the assessed functions are allocated to operator-initiated automation, predominantly (21 %) through operator-initiated sequence automation.

18.6.4 Conclusions

The AoF outputs [1] support a high level of confidence that the operator actions required by RR SMR will be reasonable and largely in-line with typical manual PWR activities, and that the limited operator actions required will be reasonable and achievable.

This confidence is due to the AoF process ensuring that any actions that require a response from the MCR within 30 minutes, or locally within 1 hour, will be screened out and those that are outside of human capabilities and strengths will be automated or supported by engineering.

This assumes that there will be suitable interfaces and that the operator will be adequately trained and supported.

Given the level of design maturity at RD7/DRP1, it cannot yet be demonstrated that all processes and actions are appropriately allocated between human and engineered function.

18.7 Identification of Operator Actions

18.7.1 Introduction

This section provides substantiation of the following hierarchy of claims:

1. 18.1.3. Human based actions enable safe and secure operation and maintenance of the RR SMR throughout the lifecycle of operation and all operating modes.

2. 18.1.3.1 The operator actions required to operate and maintain the RR SMR are identified.

3. 18.1.3.1.2 Human based actions are systematically identified.

HF assessments need to consider all human involvement with the RR SMR, whether for normal, faulted or emergency operations. A number of techniques are used to identify and assess the role of the operator; these are summarised within the HFIP [10].

A key design principle of the RR SMR is for systems to be passive or automated, which limits claims on the operator. Similarly, there is an expectation that the SMR will be 'secure by design' to limit the need for active security systems and associated security based claims on the operators. The RR SMR is a PWR, with few areas of novelty in its operation. Where novel areas exist, the opportunity to reduce the reliance on operators has been taken, for example through reducing the number of normal operational discharges to manage.

There is a high level of confidence that the operator actions required by RR SMR will be reasonable and largely in-line with typical manual PWR activities, and that the limited operator actions required will be reasonable and achievable.

Whilst increased passivity will be provided against all modes of operation, operator actions are still required to perform a number of normal operational duties during power and shutdown operations, monitor the initiation of safety systems, and contribute to the longer-term management of safety systems and emergency arrangements.

Operator actions will be identified through a number of sources, including HAZID studies, HAZOP studies, Fault Schedule, PSA and the decomposition of operator activities via TA. At RD7/DRP1, given the concept maturity, the identification of operator actions is still progressing, with those identified operator actions predominantly in support of the safety claims.

It is anticipated that the RD8 and RD9 phase will identify the majority of the remainder of the safety operator actions, with a focus on those presenting the highest level of risk to the RR SMR. The identification of detailed operator actions, particularly those in support of lower risk activities and in support of environmental, security and safeguard activities, will continue into the subsequent phase.

Through the RD7/DRP1 phase, the HF team have been represented at HAZID and HAZOP, with HF guidewords used to provide an initial list of considerations, which include references to the related HF checklist sections.

The Fault Schedule identifies a number of operator actions given there is an expectation that remote operator actions are not required for at least 30 minutes after an alarm, with local operator actions not required for at least one hour after an alarm. Further detail is provided in Section 18.7.2.

Some of the assumed operator actions stated within the Fault Schedule may be allocated to systems once the AoF process has completed, however an early review of the operator actions claimed within

the Fault Schedule has not identified any operator actions which would be challenging to demonstrate as achievable.

At RD7/DRP1, TA [4] has been developed for normal and abnormal operations and for the response to key plant faults. TA has been generated for a number of activities, notably start-up, shutdown and some refuelling activities to identify the role of the operator within these activities.

A high level TA for the 'Power Plant' has been developed, that outlines the key operator tasks grouped against the type of operation being delivered, and where applicable, the Fundamental Safety Function (FSF) that the operation supports. Overall, the 'Power Plant' TA covers 10 types of operations that will require some operator involvement, including (but not limited to) commissioning, normal, abnormal and emergency operation.

At RD7/DRP1, due to being in the early phases of the design only a limited number of systems have sufficient design information available to support generation of TA. No systems have progressed through to DD and, as such, the overall design maturity does not support the full breadth of TA development.

High level TA have also been developed for Manufacture, Build and Normal Operation including EMIT, based on the Basis of Design (BoD) TA, and further detail in relation to those activities contained in the ConOps [27]. These TA are of limited maturity given the stage of design. In total, approximately 37 TA have been created at varying levels, summarised further in the TA progress report [4].

18.7.2 Human Error Identification

Operator actions are identified from a number of sources, dependent on whether they are in support of normal or faulted operation, and the type of functions they support.

Within the phases to date, the operator actions identified have been for complex normal operations such as transitions between operating modes and safety classified systems.

Hazard Identification

During RD7/DRP1, HAZID studies have been focused on RI, TI and Balance Of Plant (BOP) based on the level of design maturity and level of risk. Subsequent phases will have more detailed HAZID studies and HAZOP studies across all islands and systems.

A SQEP HF practitioner have been on the panel for all HAZID and HAZOP to ensure integration and consideration of HF requirements. At RD7/DRP1, 37 HAZID have been attended with the majority being focused on the systems within the RI. Examples of HAZIDs that have been attended include:

- Chemical & Volume Control System (CVCS)
- Passive Decay Heat Removal (PDHR) & Local Ultimate Heat Sink (LUHS)
- Component Cooling System
- RI Waste Systems
- Scram
- Sampling Systems.

During the HAZID, 'Human Factors' is used as a guideword. This prompts discussion on HF and includes consideration of how human error/ procedural failures could occur and how they could be

mitigated. These are recorded in the hazard log and screened and may result in an associated claim being placed on an operator action.

Areas for further investigation during the subsequent design phases were noted, for example development of appropriate interfaces or controls.

Probabilistic Safety Assessment

The RR SMR PSA includes numerous operator actions, which are identified as part of the modelling process, as reported via event sequence modelling activities and SSC modelling activities. This is reported in E3S Case Version 2, Tier 1, Chapter 15: Safety Analysis [7] for further detail.

The operator actions modelled in the PSA consider the safety-related operator actions made in the deterministic case, along with additional operator actions that may be critical for the operation of the plant from a probabilistic perspective (judged as best practice).

The identification of operator actions was based on the definition of postulated initiating events and the fault schedule.

The PSA not only represents HBSC in the form of operator actions, but also identifies and claims operator actions not previously identified as HBSC, that have been reviewed by HF and recorded as new HBSC where appropriate.

Every operator action in the RR SMR PSA is related to one or multiple HBSC, and has its own dedicated description, which provides all the necessary information needed to explain, construct, and understand the base event (BE) and fault tree (FT) modelling of the operator action in the PSA model.

As a general approach, operator actions are represented within the RR SMR PSA as one or more human failure event (HFE), each represented as a BE and combined within a FT structure and assigned with an appropriate HEP.

As a safety analysis topic, the scope of operator actions in the RR SMR PSA excludes any malicious action taken with deliberate intent.

At RD7/DRP1, the PSA only considers operator actions that align to Type 3, Type 4 and Type 5 HBSCs. Detailed design information about equipment EMIT activities is not available, and therefore Type 1 HBSCs cannot be derived yet. In addition, where failure to achieve some of the Type 2 HBSC may result in a Postulated Initiating Event (PIE), these have not been derived, and therefore the complete scope of potential HFE is not yet available. As such, Type 1 and Type 2 operator actions have not been included.

Future revisions will extend the RR SMR PSA to include Type 1 and Type 2 operator actions, operator action dependencies and influencing factors, and human performance limiting value (HPLV). It will also include Level 2 and Level 3 PSA operator actions, and take into consideration hazard scenarios, maintenance, and remaining operating modes, as well as a more detailed approach for the derivation of HEP for those operator actions which fall outside the scope of the HBSC tracker.

HRA is discussed further within Section 18.8.2 and 18.8.3.

Fault Schedule

The Fault Schedule [28], and E3S Case Version 2, Tier 1, Chapter 15: Safety Analysis [7], identifies a number of explicit claims on the operator to undertake preventive safety measures and identifies protective safety systems which operators will monitor the initiation and operation of. These are assumed operator actions in support of the E3S Case; these functions continue to be assessed through the AoF methodology to determine their allocation, e.g., allocated to the operator or automated.

At RD7/DRP1, a comprehensive review of the PIE Definition and IEF Derivation Report (see E3S Case Version 2, Tier 1, Chapter 15: Safety Analysis [7] for further detail) was performed with particular focus on identifying and verifying the correct allocation of those attributed to operator error, and provided confidence that the DSA is assessing all credible faults.

To date, 443 HBSC have been derived across the full scope of operation and maintenance activities allocated to the operator. However, this total only includes generic EMIT tasks and is anticipated to develop significantly once specific EMIT tasks are fully identified for each individual system.

It is considered that the HBSC identified to support preventive safety measures are reasonable and achievable based on the simplicity of the action required (e.g., stopping a single pump from the MCR) and application of a minimum 30-minute for remote, or 1 hour for local grace period before operator action is required [29].

The protective safety measures identified in the Fault Schedule [28] will automatically initiate. The operator will be required to monitor the initiation and operation of these safety measures but is not required to actuate any controls in the early phases of the safety measure operation. Therefore, there is no claim for local to plant operator actions within the first 72 hours to protect any Loss of Electrics (LOE), Intact Circuit Fault (ICF), or Loss of Coolant Accident (LOCA).

Operator interaction will be required to complete actions beyond 72 hours to ensure the long-term operation of the safety measure. The detail and location of operator actions required 72 hours after an event and beyond are still to be defined. However, it is anticipated that most operator actions will be performed from the MCR, minimising the requirement for local to plant operator actions.

At RD7/DRP1, the actions required 72 hours after an event and beyond are still to be defined. The role of the operator in these activities will be determined during the next design phase, using techniques such as AoF.

Not all of the indications available to the operator to monitor the initiation and operation of these protective safety measures have been identified or designed yet. However, there is confidence that the appropriate controls and indications will be provided for the operators such that they can complete the actions.

The subsequent design phase will systematically assess the claims on the operator to confirm that the operator has sufficient and appropriate information, indications and controls available to them to complete the task safely.

Task Analysis

TA identifies the breadth of human-system interactions expected for operation of a power station to inform the ongoing SMR design. The human system interactions described are well understood and can be delivered with existing technologies.

The TA provides further decomposition and definition to the operator actions identified within the Fault Schedule or normal operation functional decomposition. The TA identifies the:

1. Task and sequence, for example, Task number, Task description, and sequence of operation (plan).

2. Workload and staffing, for example, Time to complete the task, a total, or running, personnel who will perform the action, and any supervision.

3. Design, for example, Location within the power station the task is performed, the type of control to perform the action, any required indication, the interface type, and specific tooling.

The substantiation of the ability of the operator to complete these actions is provided within the HBSC.

At the time of issue approximately 37 TA have been created at varying levels. These TA are summarised further in the TA progress report [4], and include:

1. High Level Power Plant Operation, for example, commissioning, normal operation, emergency operation, waste management, and fuel handling.

2. Process TA, for example, start-up, shut-down, re-fueling, and spent fuel movements.

3. System TA, for example, Passive Steam Condensing System, LUHS System, Essential Service Water System, Auxiliary Cooling and Make-up System, Fuel Pool Fluid Systems.

4. Safety Measure TA, for example, low temperature decay heat removal (LTDHR), alternative shutdown function (ASF), emergency core cooling (ECC).

TA is a multi-purpose activity, serving to contribute to the verification of the AoF and identify C&I required to support the operator at each task step. This will translate into formal requirements being placed on DD of the HMI to ensure that appropriate C&I will be provided as part of the operator interface, both within the control facilities and local to plant.

The output from TA will serve as an input to future HF work packages including identification of operator actions and HBSC. It will also provide validation of AoF whilst identifying any deviations from the intended process due to current project constraints and limitations.

18.7.3 Conclusions

The identification of operator actions has continued within this phase, with these primarily being associated with safety related systems and complex normal operational processes such as start-up. These have been identified from the Fault Schedule, PSA and TA [4]. It is anticipated that a similar process will be followed to identify any environmental, security or safeguards based claims on the operator; none have explicitly been identified so far.

The operator actions identified to date include all ‘Types’ of operator actions. Some of these are generic at this phase, with scenario specific detail expected to be available through the subsequent design phase. For example, specific EMIT operator actions will be identified in the subsequent phase as the design continues to mature.

18.8 Operator Action Substantiation

18.8.1 Introduction

This section provides substantiation of the following hierarchy of claims:

1. 18.1.3 Human based actions enable safe and secure operation and maintenance of the RR SMR throughout the lifecycle of operation and all operating modes.
2. 18.1.3.1 The operator actions required to operate and maintain the RR SMR are substantiated.
3. 18.1.3.1.1 Human based actions are substantiated.

The operator actions identified through the means discussed in the previous section require substantiation.

A sub-set of HF techniques have been applied so far, with the remaining techniques (such as cognitive workload assessment (CWA)) planned for application during the future phases of the programme as the design matures. The assessments completed within this phase are discussed within this section and Section 18.6 Allocation of Function.

These assessments are required for all operator actions, rather than only those modelled within the E3S Case. However, the assessment will be proportionate to the level of operator involvement, and the consequences of any errors.

The analysis of operator actions will need to consider the impact on staffing, e.g., number of personnel and location, job design, e.g., requirements for shift work, or multi-skilling, and training, e.g., any additional or atypical requirements. Additionally, the assessment will consider the potential for robotics, remote operations and automation which could support the operator in the delivery of their role.

As discussed within Section 18.7, the claims which have been identified so far are derived from the E3S case therefore this section discusses the methods used to substantiate safety related operator claims.

18.8.2 Qualitative Analysis

The scope of substantiation evidence requirements to support HBSC assessment will consider (depending on safety classification) demonstration that:

- There is an appropriate prompt for the action
- Sufficient indications are available for diagnosis and/or monitoring
- Suitable means are available to complete the action
- Feedback is provided after the action is completed
- There is space available to complete the action
- The environment is suitable for completion of the action

- The action can be completed within the timeframe available
- The action can be completed by the staff available
- There is a procedure or administrative control to support completion of the action
- There are suitable Safety Management Arrangements (SMA) to support completion of the action
- Staff are trained to complete the required action.

Within this phase, the reviews of operator actions have been limited in scope and detail, as the operator actions are still being identified, and the design definition doesn't currently provide sufficient information to allow for substantiation in detail. Requirements will be captured for the design to include features to enable the operator to successfully complete the claimed actions.

The TAD [2] has been available to all design teams to use in their development of concept system designs and layout configurations. The HF team has supported the application of the TAD data in determining whether the current concept layout configurations provide safe and sufficient space for personnel to complete the identified tasks, either for operations or maintenance. The layout concept is continuously developing as further design details are available. HF requirements have not been fully satisfied yet, however they will be satisfactorily incorporated through the remainder of the concept development.

Any requirements for additional tooling or shielding have been identified as part of the assessments to ensure that all aspects of a task can be safely undertaken.

As is typical for the early design phase with associated design maturity, large components have been included in CAD models whereas smaller components or structural features have not been included in all areas. The potential impact of these additional features on the space available for personnel will be considered as part of the on-going assessments.

During concept reviews and the development of the task analysis, the availability of appropriate controls and indications (including warnings or alarms) has been considered however at this design phase, not all controls and indications have been identified therefore the layout concepts don't yet include representations of controls and indications. The HF analysis has and will continue to identify the controls and indications which will be required, and early engagement with the design teams ensures that these requirements are captured.

Gracetime information is not yet available for all aspects of the plant which the operator interacts with. However as discussed within Section 18.6, the operator is not required to complete actions in support of safety systems from the MCR for at least 30 minutes or locally for 1 hour after an alarm and they are typically not required to take action until approximately 72 hours into an event.

Operating documentation and training are recognised as key elements of demonstrating that activities can be completed. They will both be progressed during the subsequent design phases, recognising that the dutyholder/licensee/permit holder will have ultimate responsibility for demonstrating to the regulators that they have the appropriate arrangements in place. See Section 18.9 for related claims and discussion.

18.8.3 Quantitative Analysis

HRA consists of a range of HF methods for identifying the contribution people make to risk. It provides a structured approach for understanding how human performance and actions can contribute to an overall risk profile by providing probabilities of human error.

This quantitative evaluation builds upon and is completed in conjunction with the qualitative task analysis and HBSC assessments which provide the detailed context around the action which is being quantitatively assessed.

The RR SMR design ensures that limited operator actions are required in the delivery of safety functions through the provision of passive or automated systems. The interaction of personnel with these passive or automated systems is assessed as part of the AoF determination (see Section 18.6 for more details).

Methodology

The structured approach consists of familiarisation, qualitative error analysis, quantitative error analysis and finally derivation refinement. As described in Section 18.8.3, the quantitative and qualitative analysis will be integrated, to ensure the quantitative analysis of actions considers the wider context of plant operation.

A PSA was conducted on the RR SMR design at RD7/DRP1. Due to the continued development of both the plant design and the safety case, the PSA is of a reduced scope and level of detail.

There are few sequences in the PSA which required an operator action to initiate a safety measure successfully. The PSA model applies a screening HEP of 1.00E-02 to all operator actions, assumed to represent the best estimate value given insufficient qualitative evidence available to derive best-estimate HEP. It is fully acknowledged that application of a HEP of 1.00E-02 to represent all operator actions does not meet the expectations for HRA.

As the design continues to mature towards RD8 and into the following design phases, a more detailed approach to the quantification of operator actions will be performed. The RR SMR HRA: Quantitative Assessment Strategy [20] provides a discussion of the potential approaches to be utilised.

RD7/DRP1 Status

A PSA has been developed to evaluate the RR SMR at power, e.g., operating modes 1 and 2, with systems in their normal duty line up prior to the occurrence of a fault. Operations with the reactor shutdown, refuelling activities and initiating events occurring within the spent fuel pool are outside of the scope of the extant PSA, as reported in the PSA Report [30].

A PSA is provided for plant faults only: ICF, LOE, and LOCA. The initiating fault definition and boundary is as defined in the RR SMR Definition of Postulated Initiating Events Report [31] . Note that hazards are out of the current scope of the PSA model and will be included in later iterations.

Only a Level 1 PSA has been developed. Level 2 and level 3 PSA will be conducted in future work, and specific comparisons against each target made.

PSA results identify that the RR SMR presents a fairly balanced design with a Core Damage Frequency (CDF) calculated as 7.56E-07 per reactor year (pry) of power operation. A review of the dominant accident sequences has been performed to understand the dominant risks from the PSA model that contain operator error. In addition, the key risk contributors have been identified that are attributed specifically to operator error.

Four operator actions are considered to present a significant contribution to risk and impact on the baseline CDF of 7.56E-07 pry. The key operator actions are:

1. Operator fails to maintain the Diesel Generator (DG) fuel tank levels beyond 72 hours in case of a Loss Of Offsite Power (LOOP) (168 hours).

2. Operator fails to manually configure the High Pressure Injection System (HPIS) in the case of a Steam Generator Tube Rupture (SGTR).

3. Operator fails to manually restart the CVCS in the case of spurious ASF initiation, or spurious HPIS initiation, faults.

4. Operator fails to manually stop the HPIS in the case of spurious HPIS initiation fault.

The dominant contributor presents a Fussell-Vesely (F-V) contribution of 33 %, suggesting that the CDF results are very sensitive to the long-term management actions associated with DG operation. The HEP currently assigned to the failure to replenish the DG fuel tanks is expected to improve when fully assessed, e.g., consideration to the extensive timescale available before operator action is required allowing the operators to anticipate and prepare for the action. Application of a more representative HEP presents the greatest opportunity to reduce the total CDF, with a high degree of confidence that this can be achieved.

The three remaining dominant operator actions present a F-V contribution of 5 %, 2 % and 2 % respectively, again suggesting that the CDF results are sensitive to these operator actions. Once again, given the limited maturity of the design and operational process associated with these scenarios, there is a high degree of confidence that as the RR SMR progresses and a detailed derivation can be provided, that the total CDF can be further reduced.

A series of sensitivity studies have been performed to assess the impact of variation in HEP screening value and ensure the risk conclusions of the PSA are robust.

The sensitivity studies considered a broad spectrum of HEP ranging from a significantly pessimistic assessment, assigning all operator actions modelled within the PSA to unity (1.00), through to a somewhat more representative and achievable sensitivity scenario of 1.00E-03 for all operator actions.

Assigning all HEP to unity increases the CDF from 7.56E-07 pry to 3.22E-05 pry, which highlights the importance of the operator and requirement to develop a design that is by predominantly passive or automated. However, it is considered significantly pessimistic to assume that all tasks requiring operator action fail.

Assigning all HEP to 1.00E-03 reduces the CDF from 7.56E-07 pry to 4.71E-07 pry, demonstrating that continued integration and influence of HF through application of the full suite of HF tools and techniques, e.g., HF checklist, AoF workshops, etc., will assist in achieving this lower bound set of HEP.

Subsequent design phases will also systematically identify and proportionately assess the full scope of HBSC across all modes of operation. This will generate evidence to substantiate the role of the operator against the full set of criteria, which will draw on the detailed design activities described above. During this process, the purpose of the TA will evolve from a tool to generate requirements to an analytical tool from which evidence can be based.

A more detailed approach to the quantification of operator actions will then be performed utilising the qualitative evidence obtained to support HBSC substantiation to support application of informed HEPs as the PSA matures, with the aim to reduce the sensitivity on any operator actions.

18.8.4 Conclusions

As discussed in Section 18.7 the identification of operator actions will continue through the RD8 and RD9 phases, and the substantiation of these will develop as the design matures. The initial operator actions have been substantiated as far as the design definition allows, for example without the detail of the specific controls and indications.

Without the scenario specific detail, screening HEP have been used within the PSA. Sensitivity studies have been applied to vary the screening HEP value, in order to evaluate the effect on the

CDF. It is anticipated that the required detail to allow detailed HEP to be derived will be available through the RD8 and RD9 phases.

It is anticipated that similar methods will be useful in substantiating operator claims for other E3S disciplines; as the claims are identified the applicability of the methods will be reviewed.

18.9 Future Dutyholder/Licensee/Permit Holder Capability

18.9.1 Introduction

This section provides substantiation of the following hierarchy of claims:

1. 18.4 The RR SMR design is informed by assumptions on the capability of a future licensee from a HF perspective.

2. 18.4.1 The RR SMR can be safely operated and maintained through-life by a future licensee's organisation.

3. 18.4.1.1 The staffing concept supports safe operation of the RR SMR.

4. 18.4.1.2 The training concept supports safe operation of the RR SMR.

5. 18.4.1.3 The procedure concept supports safe operation of the RR SMR.

Claims placed on the operator are reliant on the future licensee implementing key functions, such as the correct staffing levels, the appropriate training, and the provision of adequate procedures. Whilst it will be the future licensee who has responsibility for delivering these, RR SMR will enable the future licensee to deliver these by developing and implementing processes which generate the required information.

Assumptions and Commitments made which the future dutyholder/licensee/permit holder would be expected to deliver against to support the substantiation of operator claims are identified in the following sub-sections.

18.9.2 Staffing Concept Development

Given the design maturity at RD7/DRP1, the current staffing concept has been developed from the top-down through comparisons with existing nuclear facilities and a review of the RR SMR design concept to identify any differences in the design and operation which could influence the staffing levels. This staffing concept has been reviewed by Constellation, a current nuclear power plant operator with knowledge of UK licensing arrangements. Section 18.2.7 discusses the concept in further detail.

In the future programme phases, the TA and AoF will develop the staffing concept through identification of the tasks which personnel are required to complete, when, and from where. As more design detail is added, and more task definition is generated, a detailed review of staffing, including workload, will ensure that assigned tasks remain manageable.

From this analysis, a generic Nuclear Baseline will be identified. The Nuclear Baseline is a means by which a licensee demonstrates that its organisational structure, staffing, and competencies are, and remain, suitable and sufficient to manage nuclear safety throughout the full range of the licensee's business and plant lifecycle and for all operational states. RR SMR will develop a generic Nuclear Baseline to support an operator / licensee when taking ownership and responsibility for the design, and to provide an assumed staffing concept to be used in assessments. It is the dutyholder/licensee/permit holders responsibility to develop the site specific Nuclear Baseline.

The overall staffing concept will include personnel and skillsets additional to the Nuclear Baseline, who are likely required for the general support of the RR SMR such as outage planners, warehouse staff and crane operators.

The requirements and guidance provided within [19] regarding job design will inform the staffing concept, for example suggesting opportunities for multi-skilling of personnel where appropriate and beneficial.

Based on the above, the following Commitment is captured on the future dutyholder/licensee/permit holder:

Commitment on Future Dutyholder/licensee/permit holder C18.1: The future dutyholder/licensee/permit holder will develop a site specific nuclear baseline from the RR SMR staffing concept which supports the claims within the E3S case.

18.9.3 Training

Detailed arrangements for training staff so they can safely undertake the identified activities are the responsibility of the operator/licensee/permit holder. However, early consideration of training as part of the production of a robust staffing model is beneficial, and key to the provision of a design solution that is attractive to operators/licensees.

For example, decisions on novel technologies or alternative applications of existing technologies can have implications on the training required to deliver staff with the required knowledge, skills and attitude. Early consideration of training establishes a baseline of expected (and established) training methods and technologies and identifies opportunities for exploitation of new technologies to improve training effectiveness and efficiency.

Future phases of the programme will include a Training Needs Analysis (TNA), which is a structured process to identify training requirements and training options for a design solution. The output of the TNA is a set of training recommendations for consideration in training design, which includes selection and development of the most appropriate training medium to deliver the training recommendation.

It is likely that a recommendation from the TNA will be for a full scope training simulator of the control rooms for initial and refresher training. A control room simulator also acts as a valuable design development tool and allows for the verification of certain HF requirements. During this phase, plans for the full scope simulator have been developed.

Based on the above, the following Commitment is captured on the future dutyholder/licensee/permit holder:

Commitment on Future Dutyholder/Licensee/Permit Holder C18.2: The future dutyholder/licensee/permit holder will deliver a training programme which provides the operators with the knowledge, skills and attitudes required to support the claims within the E3S case.

18.9.4 Procedures

Procedures are not yet available for RR SMR given the design phase of the programme. TA will provide a description of operator activities, identifying the personnel, location, controls and indications, forming a pre-cursor to the procedures themselves.

Whilst the detailed procedures are not available, the type of procedures used, i.e., event or symptom based, will influence the HMI. Therefore, the HMI development will need to consider the types of procedures likely to be used for RR SMR. Through the subsequent design phases, the operating rules for RR SMR will be identified from the E3S case and collated for the future licensee.

Based on the above, the following Commitment is captured on the future dutyholder/licensee/permit holder:

Commitment on Future Dutyholder/Licensee/Permit Holder C18.3: The future dutyholder/licensee/permit holder will provide all operational staff (across all disciplines) with procedures which provide them with the required information to complete their activities in line with the requirements of the E3S case.

18.9.5 Conclusions

The claims discussed within this section cannot fully be achieved without the future dutyholder/licensee/permit holder delivering on commitments captured in this Section. The ongoing design development aims to ensure these commitments are achievable for the future dutyholder/licensee/permit holder. For example, through consideration of the HMI and how it can support the activities undertaken by the future operators.

18.10 Conclusions

18.10.1 ALARP, BAT, Secure by Design, Safeguards by Design

HF assessments are a key element of reducing risks to ALARP and supporting the Secure by Design approach. As discussed within Section 18.3, the HF Team are involved in the design development through guidance, requirements and as stakeholders for HAZID, HAZOP, Definition and Decision Reviews.

The HF assessments aim to reduce claims on the operator, through ensuring appropriate levels of automation and remote operations. The qualitative and quantitative assessments discussed within Section 18.6 and 18.8 demonstrate the RR SMR design is limiting claims on the operator, particularly for the initiation of any safety measures.

18.10.2 Assumptions & Commitments on Future Dutyholder/ Licensee / Permit Holder

Table 18.10-1: Assumptions and Commitments on Future Dutyholder/Licensee/Permit Holder

Assumption/Commitment	ID	Description
Commitment	18.1	The future dutyholder/licensee/permit holder will develop a site specific nuclear baseline from the RR SMR staffing concept which supports the claims within the E3S case
Commitment	18.2	The future dutyholder/licensee/permit holder will deliver a training programme which provides the operators with the knowledge, skills and attitudes required to support the claims within the E3S case
Commitment	18.3	The future dutyholder/licensee/permit holder will provide all operational staff (across all disciplines) with procedures which provide them with the required information to complete their activities in line with the requirements of the E3S case

18.10.3 Conclusions and Forward Look

Given the early stage of the design development it has not been possible at this time to confirm that all HF claims have been substantiated as greater design definition is required in addition to some areas of testing. However, the analysis of the current concept provides confidence that it will be possible to substantiate the HF claims at an appropriate stage in the design and safety case, as the design continues to mature and as HF guidance continues to be embedded.

HF has been integrated with the design since the commencement of the RR SMR design. Multiple forms of guidance have been generated to inform and support the design teams and empower them to incorporate HF guidance independently with HF confirming the application. This allows the HF Team to prioritise their focus on more complex, and higher safety classified components and systems.

The primary assessments to date have been AoF and TA, with limited application of HRA, both qualitative and quantitative. These have been, and continue to be, used to assess the design at various stages. They have aimed to optimise the role of the operator, reducing the reliance on the operator and reducing any risks to ALARP.

The HRA completed to date has demonstrated there are limited sequences in the PSA which the operator is a dominant contributor to. Whilst the sensitivity studies demonstrate the CDF is currently sensitive to the operator contribution to these events, there is still the ability to significantly influence the design including increased automation or remote operation. Additionally, assessing these operator actions in detail, rather than with screening HEP, is expected to reduce the pessimism within some of these calculations.

HF are continuing to inform and assess the design as it continuously evolves. Through the next phase of the design, there will be further assessments of the layout including the control facilities. As the TA increases in detail, specific C&I requirements will be identified, allowing for the HMI for the primary control facilities such as the MCR, SCR and ERC to be developed. Operational experience will be reviewed to generate appropriate guidance and to inform the design development.

Specific EMIT related operator actions will be developed in the subsequent phases, further supporting the layout development by identifying the key actions required in each location and the respective space envelopes needed for personnel.

As the generic E3S Case is developed to meet its objective ‘to provide confidence that the RR SMR design will be capable of delivering the E3S fundamental objective as it developed from a concept design into a detailed design’ [8], further arguments and evidence to underpin the claim will be developed in line with the E3S Case Route Map [9] and reported in future revisions of the generic E3S Case throughout Step 3.

18.11 References

[1] Rolls-Royce SMR Limited, SMR0005768/003, “Allocation of Function Summary Report,” December 2023.

[2] Rolls-Royce SMR Limited, SMR0003975, “Target Audience Description,” January 2023.

[3] Rolls-Royce SMR Limited, SMR0003911/001, “Human Machine Interface (HMI) Style Guide,” December 2022.

[4] Rolls-Royce SMR Limited, SMR0009105, “Task Analysis Progress Report,” December 2023.

[5] Rolls-Royce SMR Limited, SMR0005883/002, “Control Facilities Description,” December 2023.

[6] Rolls-Royce SMR Limited, SMR00004366/001, “RR SMR Human Reliability Analysis Strategy,” February 2023.

[7] Rolls-Royce SMR Limited, SMR0003977/003, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 15: Safety Analysis, May 2024.

[8] Rolls-Royce SMR Limited, SMR0004294/003, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 1: Introduction, May 2024.

[9] Rolls-Royce SMR Limited, SMR0002155/003, E3S Case Route Map, November 2023.

[10] Rolls-Royce SMR Limited, SMR0000219, “Human Factors Integration Plan,” March 2023.

[11] BS EN ISO 6385, Ergonomic Principles in the Design of Work Systems, September 2016.

[12] Rolls-Royce SMR Limited, SMR0005213/001, “Power Station Operating Philosophy,” July 2023.

[13] Rolls-Royce SMR Limited, SMR0004599/003, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 21: Decommissioning and End Of Life Aspects, May 2024.

[14] Rolls-Royce SMR Limited, SMR0007559, Staffing Concept, August 2023.

[15] Rolls-Royce SMR Limited, EDNS1000896665/001, “Level 0 SMR Requirements,” April 2021 (Live version in DOORS).

[16] Rolls-Royce SMR Limited SMR0008444/001, Approach to Verification and Validation, December 2023.

[17] Rolls-Royce SMR Limited, EDNS01000925953/001, “Accomodation of Humans into the Built Environment,” November 2020.

[18] Rolls-Royce SMR Limited, EDNS01000925954_001, “Minimising Human Error,” November 2020.

[19] Rolls-Royce SMR Limited, EDNS01000925955/001, “Staffing, Job Design and Training,” November 2020.

[20] Rolls-Royce SMR Limited, SMR00004028/001, “RR SMR Human Reliability Analysis: Quantitaive Assessment Strategy,” January 2023.

[21] Rolls-Royce SMR Limited, SMR0007096, *Infrequent Corridor Permitted Non-Compliance - Ducking,* July 2023.

[22] Rolls-Royce SMR Limited SMR0004571/003, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 19: Emergency Preparedness and Response, May 2024.

[23] Rolls-Royce SMR Limited, EDNS01000533897, “Small Modular Reactor Control Rooms Outline Description,” December 2017.

[24] M.Endsley, “Level of Automation Effects on Performance, Situation Awareness and Workload in a Dynamic Control Task,” *Ergonomics,* vol. 42, no. 3, pp. 462-492, 1999.

[25] EPRI, “HFAM - Human FActors Analysis methodology for Digital Systems,” November 2021.

[26] Rolls-Royce SMR Limited, SMR0003673, “Design Maturity Timeline,” January 2023.

[27] Rolls-Royce SMR Limited, SMR0005048/001, “Concept of Operations,” March 2023.

[28] Rolls-Royce SMR Limited, SMR0004444/006, Fault Schedule, March 2023.

[29] Office for Nuclear Regulation, NS-TAST-GD-010 – Early Initiation of Safety Systems, December 2022.

[30] Rolls-Royce SMR Limited, SMR0008550/001, “Probabilistic Safety Assessment (PSA) Main Report,” January 2024.

[31] Rolls-Royce SMR Limited, SMR0001389 Issue 3, “Definition of Postulated Initiating Events and Derivation of Initiating Event Frequencies,” April 2023.

18.12 Appendix A: Claims, Arguments, Evidence

Table 18.12-1 provides a mapping of the claims to the corresponding sections of the chapter that summarise the arguments and/or evidence. The full decomposition of claims and link to underpinning Tier 2 and Tier 3 information containing the detailed arguments and evidence is presented in the E3S Case Route Map [9].

Table 18.12-1: Mapping of Claims to Chapter Sections

Claim	**Section of Chapter 18 containing Arguments / Evidence summary**
A suite of HF activities are carried out to integrate HF into the RR SMR design	18.3
HF requirements are derived from principles, standards, RGP and OPEX	18.3
A suitable RR SMR Target Population is defined	18.4
The RR SMR target population is accommodated in the design	18.4
Controls and Indications are provided for the operator	18.5
The layout of RR SMR enables safe and reliable performance of the operator through-life and through all operating modes	18.5
Processes and actions are appropriately allocated between machine and operator	18.6
Human based actions are systematically identified	18.7
Human based actions are substantiated	18.8
The staffing concept supports safe operation of the RR SMR	18.9
The training concept supports safe operation of the RR SMR	18.9
The procedure concept supports safe operation of the RR SMR	18.9

18.13 Abbreviations

ALARP	As Low As Reasonably Practicable
AoF	Allocation of Function
ASF	Alternative Shutdown Function
BAT	Best Available Technique
BE	Base Event
BoD	Basis of Design
BOP	Balance Of Plant
C&I	Control and Instrumentation
CAD	Computer Aided Design
CAE	Claims, Arguments, Evidence
CDF	Core Damage Frequency
ConOps	Concept of Operations
COTS	Commercial Off The Shelf
CVCS	Chemical & Volume Control System
CWA	Cognitive Workload Assessment
DD	Developed Design
DG	Diesel Generator
DR	Design Review
DR	Definition Review
DRP1	Design Reference Point 1
DSA	Deterministic Safety Assessment
E3S	Environmental, Safety, Security and Safeguards
ECC	Emergency Core Cooling
EMIT	Examination, Maintenance, Inspection and Testing
EPRI	Electrical Power Research Institute
ERC	Emergency Response Centre

FAT	Factory Acceptance Testing
FC	Functional Characterisation
FSF	Fundamental Safety Function
FT	Fault Tree
FTE	Full Time Equivalent
F-V	Fussell-Vesely
GDA	Generic Design Assessment
HAZID	Hazard Identification
HAZOP	Hazard and Operability
HBSC	Human Based Safety Claims
HBSyC	Human Based Security Claims
HEP	Human Error Probability
HF	Human Factors
HFE	Human Failure Event
HFI	Human Factors Integration
HFIP	Human Factors Integration Plan
HMI	Human Machine Interface
HPIS	High Pressure Injection System
HPLV	Human Performance Limiting Value
HRA	Human Reliability Assessment
ICF	Intact Circuit Fault
LoA	Level of Automation
LOCA	Loss Of Coolant Accident
LOE	Loss of Electrics
LOOP	Loss Of Offsite Power
LTDHR	Low Temperature Decay Heat Removal
LUHS	Local Ultimate Heat Sink

MCR	Main Control Room
MEP	Mechanical, Electrical and Plumbing
OCC	Outage Control Centre
OLC	Operating Limits and Conditions
OPEX	Operating Experience
OSC	Operational Support Centre
PDHR	Passive Decay Heat Removal
PIE	Postulated Initiating Event
PPE	Personal Protective Equipment
pry	per reactor year
PSA	Probabilistic Safety Assessment
PWR	Pressurised Water Reaction
RAIDO	Risks Assumptions Issues Dependencies and Opportunities
RD	Reference Design
RGP	Relevant Good Practice
RI	Reactor Island
RR	Rolls-Royce
RWCR	Radioactive Waste Control Room
SCR	Supplementary Control Room
SDD	System Design Description
SGTR	Steam Generator Tube Rupture
SMA	Safety Management Arrangements
SMDD	Safety Measure Design Description
SMR	Small Modular Reactor
SQEP	Suitably Qualified and Experienced Personnel
SSC	Structures, Systems and Components
SyCC	Security Control Centre
TA	Task Analysis
TAD	Target Audience Description

TI	Turbine Island
TNA	Training Needs Analysis
TSC	Technical Support Centre
UK	United Kingdom
V&V	Verification and Validation
VR	Virtual Reality