|  |
| --- |
|  |
| ONR assessment report  Generic design assessment of the Rolls Royce SMR – Step 2 assessment of Control and Instrumentation |



ONR assessment report

**Project name**: Generic design assessment of the Rolls-Royce SMR

**Report title**: Step 2 assessment of Control and Instrumentation

**Authored by**: [Redacted]

**Report issue no**: 1

**Document ID**: ONRW-2126615823-2965

**Publication date**: Jul-24

© Office for Nuclear Regulation, 2024

For published documents, the electronic copy on the ONR website remains the most current publicly available version and copying or printing renders this document uncontrolled. If you wish to reuse this information visit [www.onr.org.uk/copyright](http://www.onr.org.uk/copyright) for details.

# Executive summary

This report presents the outcomes of my control and instrumentation (C&I) assessment of the Rolls-Royce small modular reactor (SMR), as part of Step 2 of the Office for Nuclear Regulation (ONR) generic design assessment (GDA). My assessment is based upon the information presented in version 2 of Rolls-Royce SMR Limited’s (the requesting party’s) environmental, safety, security and safeguards (E3S) case and supporting documentation.

ONR’s GDA process is to apply a step-wise assessment, which increases in detail as the project progresses. The focus of Step 2 was the fundamental adequacy of the design and the safety case, and the suitability of the methods, approaches, codes and standards that form the building blocks for the design and the safety case.

I targeted my assessment, in accordance with my assessment plan, at the content most relevant to C&I against the expectations of ONR’s safety assessment principles, technical assessment guides and other guidance that ONR regards as relevant good practice. My assessment has considered:

* High-level principles that establish overall design objectives for the C&I systems in their contribution to nuclear safety.
* Reference standards and guidance.
* Method for categorising safety functions and classifying safety systems.
* C&I architecture to ensure defence-in-depth; accounting for single failure criterion, common cause failure, segregation, redundancy, diversity and probabilistic reliability claims.
* C&I functional and property claims and their allocation to C&I systems.
* C&I system safety demonstration plans.
* Essential supporting systems.
* Cyber security risks to safety.

The conclusions of my assessment are as follows.

* The requesting party’s (RP’s) design principles are complete at a high level and demonstrate good alignment with ONR’s expectations for overall design goals. It is unclear at this stage how the principles will be carried through in the E3S case to provide a clear trail from claims through arguments to evidence.
* The RP’s documented set of C&I reference standards and guidance provides an appropriate benchmark for relevant good practice, with reasonable gradation in how compliance will be demonstrated. The set of internal C&I standards, still to be created by the RP, will need to capture all relevant good practice for both product and process requirements.
* The RP’s method for categorisation and classification is largely consistent with relevant good practice and has been applied appropriately in the design so far.
* The RP has identified an appropriate set of reactor C&I safety systems, with system integrity targets consistent with their classes, although the 1E-3 pfd/per year targets for the class 2 systems will require a stronger safety demonstration than the default for class 2. The high level architecture has the potential to achieve the necessary system independence. The single failure criterion is met in principle for this stage of the design.
* The use of a hardwired class 1 diverse protection system has strong potential to provide an effective means of achieving independence from the class 2 reactor protection system for defence-in-depth. It reinforces up-to-date relevant good practice for nuclear power plants in the UK, illustrating the reasonable practicability of a hardwired C&I protection system to reduce nuclear risk.
* The RP has established an adequate framework for C&I functional and property claims, but demonstration of completeness requires further development of E3S case arrangements. From a C&I perspective, these arrangements and application of claims, arguments and evidence will need improving to enable the RP to provide a coherent C&I safety demonstration.
* Safety demonstration plans for C&I systems are incomplete, but present a credible initial framework for determining an adequate set of methods and techniques for generating the evidence to support claims for each system.
* Requirements and indicative high-level architecture for essential systems for C&I, namely electrical power supplies and heating, ventilation and air conditioning, meet ONR expectations for C&I at this stage of the design.
* The RP’s application of its secure by design method in using a hardwired class 1 diverse protection system is an exemplar, considerably reducing the risk of any cyber attack leading to unacceptable radiological consequences.
* The RP has sufficiently met ONR expectations for cyber security risk assessment, accounting for a commitment to develop a method for assessing the validity of independence claims for multiple systems considering foreseeable cyber security compromise. The RP’s method for assigning security degrees is potentially inconsistent in relation to safety classification and will need demonstrating through examples of practical application.
* The RP’s principles for co-ordinating safety and cyber security progresses relevant good practice and is a good basis for plans to meet requirements. This will include combined C&I system safety and security demonstration plans to define methods and techniques for finding and resolving cyber security vulnerabilities introduced during software development of the relevant systems.

Overall, based on my assessment to date, and subject to the provision and assessment of suitable and sufficient supporting evidence, I have not identified any fundamental safety shortfalls that could prevent ONR permissioning the construction of a power station based on the generic Rolls-Royce SMR design.

# List of abbreviations

ALARP as low as is reasonably practicable

AMS accident management system

BS British standard

C&I control and instrumentation

CAE claims arguments evidence

CS&IA cyber security and information assurance

DICWG digital instrumentation and control working group

DPS diverse protection system

DPSMS diverse protection system monitoring system

E3S environment, safety, security and safeguards

GDA generic design assessment

HDL hardware description language

HVAC heating, ventilation and air conditioning

IAEA International Atomic Energy Agency

ICBM independent confidence building measure

IEC International Electrotechnical Commission

IET Institution of Engineering and Technology

MDEP multinational design evaluation programme

NEA Nuclear Energy Agency

ONR Office for Nuclear Regulation

PAMS post-accident management system

PE production excellence

pfd probability of failure on demand

PWR pressurised water reactor

RP requesting party

RPCMS reactor plant control and monitoring system

RPCS reactor plant control system

RPMS reactor plant monitoring system

RPS reactor protection system

SAMS severe accident management system

SAP safety assessment principle

SDD system design description

SMDD safety measure design description

SMR small modular reactor

SSC structure, system and/or component

SSG specific safety guide

SSR specific safety requirements

TAG technical assessment guide

TF SCS regulatory task force on safety critical software

TR technical report

TSC technical support contractor

UK United Kingdom

WENRA Western European Nuclear Regulators’ Association

Contents

[Executive summary 3](#_Toc166515356)

[List of abbreviations 6](#_Toc166515357)

[1. Introduction 8](#_Toc166515358)

[2. Assessment standards and interfaces 11](#_Toc166515359)

[3. Requesting party’s submission 14](#_Toc166515360)

[4. ONR assessment 20](#_Toc166515361)

[5. Conclusions 39](#_Toc166515362)

[References 42](#_Toc166515363)

[Appendix 1 – Relevant SAPs considered during the assessment 50](#_Toc166515364)

# Introduction

1. This report presents the outcomes of my control and instrumentation (C&I) assessment of the Rolls-Royce small modular reactor (SMR) as part of Step 2 of the Office for Nuclear Regulation (ONR) generic design assessment (GDA). This assessment is based upon the information presented in version 2 of Rolls-Royce SMR Limited’s environmental, safety, security and safeguards (E3S) case chapters (refs [1], [2], [3], [4] and [5]) and supporting documentation.
2. I carried out my assessment in accordance with the requirements of the Office for Nuclear Regulation (ONR) management system, following ONR’s guidance on the mechanics of assessment, NS-TAST-GD-096 (ref. [6]). I used the ONR safety assessment principles (SAPs) (ref. [7]), together with supporting technical assessment guides (TAGs) (ref. [8]), as the basis for this assessment.
3. This is a major report (as defined in NS-TAST-GD-108 (ref. [9])).
   1. Background
4. The ONR’s GDA process (ref. [10]) calls for a step-wise assessment of the requesting party's (RP’s) submissions with the assessments increasing in detail as the project progresses. Rolls-Royce SMR Limited is the RP for the GDA of the Rolls-Royce SMR design.
5. In April 2022, ONR, together with the Environment Agency and Natural Resources Wales, began Step 1 of the GDA for the generic Rolls-Royce SMR design. Step 1, which is the preparatory part of the design assessment process and mainly associated with initiation of the project and preparation for technical assessment in later steps, was successfully completed in 12 months.
6. Step 2 commenced in April 2023. This is the first substantive technical assessment step. The focus of ONR’s assessments in this step is towards the fundamental adequacy of the design and safety and security cases, and the suitability of the methodologies, approaches, codes, standards and philosophies which form the building blocks for the design and generic safety and security cases. The objective is to undertake an assessment of the design against regulatory expectations to identify any fundamental safety or security shortfalls that could prevent ONR permissioning the construction of a power station based on the design.
7. Prior to the start of Step 2, I prepared a detailed assessment plan for C&I (ref. [11]). This has formed the basis of this assessment and was also shared with the RP to maximise openness and transparency.
8. This report is one of a series of assessments which support ONR’s overall judgements at the end of Step 2 which are recorded in the Step 2 summary report (ref. [12]).
   1. Scope
9. The assessment documented in this report is based upon the E3S case for the Rolls-Royce SMR as summarised in the E3S case chapters and supporting documentation.
10. The overall scope of the Rolls-Royce SMR GDA is described in (ref. [13]). Rolls-Royce SMR Limited has indicated that it intends to complete a three-step GDA, with the objective of receiving a design acceptance confirmation from ONR, and has aligned its GDA scope with this objective. The GDA scope defines the generic plant and layout and includes: all systems, structures and components that are identified as being important to safety, security and safeguards; all modes of operation; and all stages of the plant lifecycle.
11. However, given the step-wise assessment during GDA, information has not been submitted during Step 2 for all aspects within the GDA scope. The following aspects of the E3S case are therefore out of scope of this assessment:

* C&I systems other than reactor C&I safety systems, that is class 1 and 2 systems on the reactor island, and the class 3 reactor plant control and monitoring system and severe accident management system.
* C&I design aspects beyond reference standards, functional and non-functional requirements and high level architecture.

1. My assessment has considered the following aspects:

* High-level principles that establish overall design objectives for the C&I systems in their contribution to nuclear safety.
* Reference standards and guidance.
* Method for categorising safety functions and classifying safety systems.
* C&I architecture to ensure defence-in-depth; accounting for single failure criterion, common cause failure, segregation, redundancy, diversity and probabilistic reliability claims.
* C&I functional and property claims and their allocation to C&I systems.
* C&I system safety demonstration plans.
* Essential services and systems (heating ventilation and air conditioning (HVAC) and electrical).
* Cyber security risks to safety.

# Assessment standards and interfaces

1. For ONR, the primary goal of the GDA Step 2 assessment is to reach an independent and informed judgment on the adequacy of a preliminary safety, security and safeguards case for the reactor technology being assessed.
2. ONR has a range of internal guidance to enable inspectors to undertake a proportionate and consistent assessment of such cases. This section identifies the standards which have been considered in this assessment.
3. This section also identifies the key interfaces with other technical topic areas.
   1. Standards
4. The ONR SAPs (ref. [7]) constitute the regulatory principles against which the RP’s case is judged. Consequently, the SAPs are the basis for ONR’s assessment and have therefore been used for the Step 2 assessment of the Rolls-Royce SMR.
5. The International Atomic Energy Agency (IAEA) safety standards (ref. [14]) and nuclear security series (ref. [15]) are a cornerstone of the global nuclear safety and security regime. They provide a framework of fundamental principles, requirements and guidance. They are applicable, as relevant, throughout the entire lifetime of facilities and activities.
6. Furthermore, ONR is a member of the Western European Nuclear Regulators Association (WENRA). WENRA has developed reference levels (ref. [16]), which represent good practices for existing nuclear power plants, and safety objectives for new reactors (ref. [17]).
7. The relevant SAPs, IAEA standards and WENRA reference levels are embodied and expanded on in the TAGs (ref [8]). The TAGs provide the principal means for assessing the C&I aspects in practice.
   * 1. Safety assessment principles
8. A list of the SAPs used in this assessment is recorded in Appendix 1. Section 4 describes how these have been applied.
   * 1. Technical assessment guides
9. The following TAGs have been used as part of this assessment:

* NS-TAST-GD-003 – Safety systems (ref. [18])
* NS-TAST-GD-005 – Regulating duties to reduce risk to ALARP (ref. [19])
* NS-TAST-GD-046 – Computer based safety systems (ref. [20])
* NS-TAST-GD-094 – Categorisation of safety functions and classification of structures, systems and components (ref. [21])
* NS-TAST-GD-096 – Guidance on mechanics of assessment (ref. [6])
  + 1. National and international standards and guidance

1. The following international standards and guidance have been used as part of this assessment:

* IAEA SSR-2/1, Safety of nuclear power plants: Design, SSR-2/1 (ref. [22])
* IAEA SSG-30, Safety classification of structures, systems and components in nuclear power plants (ref. [23])
* IAEA SSG-39, Design of instrumentation and control systems for nuclear power plants, SSG-39 (ref. [24])
* IEC 61226, Nuclear power plants – Instrumentation, control and electrical power systems important to safety – Categorisation of functions and classification of systems (ref. [25])
* Regulator task force on safety critical software (TF SCS) – Licensing of safety critical software for nuclear reactors – Common position of international nuclear regulators and authorised technical support organisations (ref. [26])
* IET code of practice – Cyber security and safety (ref. [27])
  1. Integration with other assessment topics

1. To enable my C&I assessment I worked closely with other topics. Similarly, other assessors sought input from my assessment. These interactions are key to the success of GDA to prevent or mitigate any gaps, duplications or inconsistencies in ONR’s assessment.
2. The key interactions with other topic areas were as follows.

* Fault studies assesses requirements for C&I systems, with respect to the hazards and faults they are designed to address, including the categorisation of safety functions and classification of C&I systems, and that C&I system failures are appropriately accounted for.
* Cyber security assesses the resilience of the design, with respect to cyber security threats and vulnerabilities, to ensure C&I systems operate dependably when needed. C&I supports cyber security by assessing the validity and application of necessary knowledge of the C&I safety systems for this objective.
* Electrical engineering assesses whether essential electrical services remain available for C&I safety systems. Substantiation of computer-based electrical systems, such as smart protection relays, will rely on C&I assessment.
* Mechanical engineering assesses whether dependable HVAC maintains a suitable operating environment for the C&I safety systems, and is also the lead topic for the assessment of many of the sensors and actuators used by these systems.
* Internal and external hazards assess risks to C&I operation, including potential compromises to assumed redundancy and independence.
  1. Use of technical support contractors

1. During Step 2 I have not engaged technical support contractors to support my assessment of the C&I aspects of the Rolls-Royce SMR.

# Requesting party’s submission

1. Rolls-Royce SMR Limited submitted a series of E3S chapters, or summary reports, and other supporting references, which outline the E3S case for the generic Rolls-Royce SMR design. This section presents a summary of the RP’s safety case for C&I at this stage. It also identifies the documents submitted by the RP which have formed the basis of my C&I assessment of the Rolls-Royce SMR.
   1. Summary of the Rolls-Royce SMR design
2. The generic Rolls-Royce SMR design is a three loop pressurised water reactor (PWR) with a target electrical power output of 470 MWe (from a thermal power of 1,358 MWth) and a design life of 60 years for non-replaceable components.
3. The RP developed the Rolls-Royce SMR design based upon established PWR technology, in use all over the world. Innovation comes in the form of its modular approach to construction which would see the majority of the power station built in factory conditions and assembled on site.
4. The reactor itself is of a typical PWR design, including a steel reactor pressure vessel holding fuel assemblies, steam generators, reactor coolant pumps and piping, all held within a steel containment vessel. The reactor is equipped with supporting systems for normal operations and safety measures, including C&I protection systems, which provide cooling, control criticality and contain radioactivity under fault conditions. The RP’s design philosophy is to prefer passive safety features to active components.
   1. E3S case approach and structure
5. Rolls-Royce SMR Limited has chosen to combine its cases in a holistic environment, safety, security and safeguards (E3S) case. The overall objective for the E3S case is to demonstrate that the design will ‘protect people and the environment from harm’.
6. The case made for each of the E3S purposes (environment, safety, security and safeguards) will inevitably be different at the top level, but it will draw upon common evidence outputs (as well as other non-common outputs) to substantiate each of the purposes. The RP states this will benefit clarity, integration and its understanding of impacts from any changes to the case.
7. The E3S case is being developed using a three-tier hierarchy, incorporating a claim arguments evidence (CAE) structure with the highest-level claims being derived from the RP’s own E3S principles. The highest level of the three tiers is the RP’s tier 1 E3S chapters, with the lower tiers providing more detailed arguments and evidence. This is illustrated in Figure 1.

****

Figure 1: Claim arguments evidence (CAE) structure within the E3S hierarchy (ref. [1])

1. The structure of the E3S case aims to align with the IAEA guidance for safety cases, SSG-61 (ref. [28]), supplemented to include UK specific expectations and expanded to include the other E3S purposes.
   1. Summary of the requesting party’s E3S case for C&I
2. The aspects covered by the Rolls-Royce SMR safety case in the area of C&I, broadly grouped under the eight matters I targeted in my Step 2 assessment plan (see paragraph ‎12) plus overall consideration of ALARP, are summarised below.
   * 1. Design principles
3. The RP has presented design principles for all technical aspects together in one document (ref. [29]). The principles relevant to C&I are derived mainly from IAEA requirements (particularly SSR-2/1, ref. [22]) and ONR SAPs (ref. [7]). Coverage includes initiating events, fault sequences, levels of defence-in-depth, hierarchy of controls, categorisation of functions, classification of systems, independence, cyber security, measuring plant status, engineered protection, alarms, control rooms, human factors, codes and standards, qualification, commissioning, operations, examination maintenance inspection and testing, ageing and degradation, ALARP, numerical targets, deterministic methods and safety analysis.
   * 1. Reference standards and guidance
4. The RP has defined three categories of C&I standards and guidance that determine the extent to which it will achieve and demonstrate compliance:
   1. Adopted – proof of compliance is required for all requirements, except where there is a signed-off justification for any non-compliances.
   2. Referenced – proof of compliance is required for all requirements, except where non-compliance is indicated by a justification (of less rigour than for adopted standards).
   3. Informative – guidance will be used as needed, with no justification for non-compliance.
5. Twenty IEC standards are listed as adopted, 52 standards/guidance as referenced and 80 guidance documents (such as IAEA technical reports) as informative (ref. [30]).
   * 1. Categorisation and classification
6. The RP’s method for categorisation and classification (ref. [31]) sets out how functions are assigned a safety category A, B or C, and systems are assigned a safety class 1, 2 or 3, in line with the requirements of IAEA SSG-30 (ref. [23]) and IEC 61226 (ref. [25]).
   * 1. C&I architecture
7. The RP’s objectives and design rules including defence-in-depth, described in chapter 3 of the E3S case (ref. [2]), determine the C&I reactor control and protection system architecture. Chapter 7 of the E3S case (C&I, ref. [3]), and the overall system design description for reactor island control and protection (ref. [32]), present this C&I architecture and describe how it meets the objectives.
8. The RP has produced system design descriptions (SDDs) for the following C&I systems; however, apart from for the reactor protection system (ref. [33]) and the diverse protection system (ref. [34]), these are all “high level” versions which provide limited design detail.

* Reactor plant control system (part of the reactor plant control and monitoring system).
* Reactor plant monitoring system (part of the reactor plant control and monitoring system).
* Reactor protection system (RPS).
* Diverse protection system (DPS).
* Accident management system (consisting of the post-accident monitoring system and the severe accident monitoring system).
* Upper level control system.
* Feedwater, steam and condensate control and protection system.
* Cooling water island control and protection system.
* Fuel route C&I system.
* Radioactive waste management system C&I.
* Turbine island control and protection system.

1. The RP has also produced safety measure design descriptions (SMDDs) that describe the analysis leading to the definition of key safety functions implemented by C&I for control of reactivity and control of fuel temperature. The documents also describe the structures, systems and components necessary for the functions to operate successfully and will eventually provide an overview of the demonstration that they meet their functional and non-functional requirements. The SMDDs particularly relevant to reactor C&I safety systems cover scram (ref. [35]), emergency core cooling (ref. [36]), passive decay heat removal (ref. [37]) and alternative shutdown function (ref. [38]).
   * 1. C&I functional and property claims
2. High-level functional and property claims are captured in the E3S case (see ‎3.2 and ‎3.3.6), with supporting claims documented as E3S requirements in the RP’s requirements management database. The RP has produced snapshots of the requirements for C&I systems (ref. [39] for example), although these do not distinguish E3S requirements. Safety functions implemented by C&I are detailed in the C&I engineering schedule (ref [40]).
   * 1. Safety demonstration
3. The RP’s E3S case sets out a claims arguments evidence (CAE) structure for the safety demonstration. Chapter 1 (introduction, ref. [1]) presents the top level claims, which are supported by all the other chapters, each of which has its own head CAE structure documented in the RP’s CAE route map (ref. [41]). The C&I chapter (ref. [3]) contains the high-level C&I claims, which will be supported by safety plans for the reactor C&I safety systems.
   * 1. Essential services
4. Two essential services are identified for reactor C&I safety systems – electrical power supply and heating, ventilation and air conditioning (HVAC). The RP has provided an overview of the adequacy of these services from a C&I perspective (ref. [42]).
   * 1. Cyber security for safety
5. Cyber security is included as part of the generic security report, which is chapter 32 of the E3S case (ref. [5]). The RP’s secure by design method (ref. [43]) aims to eliminate or reduce cyber security risks to safety through effective early design decisions. Cyber security risks will be assessed (ref. [44]) and control sets implemented to reduce the risks to an acceptable level.
   * 1. ALARP
6. In addition to demonstration of ALARP through application of relevant good practice, chapter 24 of the E3S case (ref. [4]) provides an overall argument, covering decision making, defence-in-depth, key design features and safety analysis, but with little detail specific to C&I.
   1. Basis of assessment: requesting party’s documentation
7. The principal documents that have formed the basis of my C&I assessment of the E3S case are:

* E3S design principles (ref. [29]).
* C&I codes and standards selection report (ref. [30]).
* E3S categorisation and classification method (ref. [31]).
* E3S case chapter 3 – Objectives and design rules (ref. [2]).
* E3S case chapter 7 – Instrumentation and control (ref. [3]).
* CAE route map (ref. [41]).
* System design descriptions (refs [32], [33] and [34]) and safety measure design descriptions (refs [35], [36] and [37]).
* C&I engineering schedule (ref. [40]).
* Safety demonstration plans (refs [45], [46], [47] and [48]).
* Support services summary (ref. [42]).
* Cyber security risk assessment method (ref. [44]) and its trial application (ref. [49]).

1. The documentation is consistent with the design reference report (ref. [50]), and the C&I supporting documentation is consistent with its reference E3S chapter 7.

# ONR assessment

* 1. Assessment strategy

1. My assessment has followed the GDA Step 2 assessment plan for C&I (ref. [11]), covering the target matters identified in the plan and repeated in the scope above (see paragraph ‎12).
2. I have taken a sampling approach to my assessment to inform my judgement on the adequacy of the RP’s submissions, in line with ONR policy (ref. [6]).
   1. Assessment
      1. Design principles
3. I reviewed the RP’s E3S design principles (ref. [29]), against the benchmark of IAEA requirements (ref. [22]), ONR’s SAPs (ref. [7]) and consultation on ONR’s experience of which technical principles are foundational to the success of the C&I design and the technical objectives covered by my C&I assessment, informed for example by previous GDAs. My conclusion is that the RP’s design principles are complete at a high level and demonstrate good alignment in overall design goals with ONR’s expectations.
4. The RP states that the principles are translated to E3S requirements, which will be tracked in a requirements management system to facilitate traceability and closeout. The RP considers the E3S requirements to be equivalent to claims in its CAE-structured safety demonstration. I judge this to be an appropriate use of the principles, which should contribute towards a comprehensive case. However, to date the RP has not provided visibility of its full claim structure to the level of E3S requirements. It is unclear how this structure will be effectively documented and communicated in the E3S case to provide a clear trail from claims through arguments to evidence (see also ‎4.2.6). This will be a key aspect of my assessment in Step 3.
   * 1. Reference standards and guidance
5. The RP identifies the following C&I standards as adopted (ref. [30]):

* IEC 61513, General requirements for systems (ref. [51]).
* BS EN 60880, Software aspects for computer-based systems performing category A functions (ref. [52]).
* IEC 62138, Software aspects for computer-based systems performing category B or C functions (ref. [53]).
* IEC 60987, Hardware requirements for computer-based systems (ref. [54]).
* IEC 62566, Development of HDL-programmed integrated circuits for systems performing category A functions (ref. [55]).
* IEC 62566-2, Development of HDL-programmed integrated circuits for systems performing category B or C functions (ref. [56]).
* IEC 61226, Categorisation of functions and classification of systems (ref. [25]).
* IEC 62340, Requirements for coping with common cause failure (ref. [57]).
* IEC 60709, Separation (ref. [58]).
* IEC 62342, Management of ageing (ref. [59]).
* IEC 62671, Selection and use of industrial digital devices of limited functionality (ref. [60]).
* IEC 60780-323, Electrical equipment important to safety – Qualification (ref. [61]).
* IEC 60980-344, Equipment important to safety – Seismic qualification (ref. [62]).
* IEC 60964, Control rooms – Design (ref. [63]).
* IEC 61000-4 parts 1-6, Electromagnetic compatibility – Testing and measurement techniques (refs [64], [65], [66], [67], [68] and [69]).
* IEC 62645, Cybersecurity requirements (ref. [70]).
* IEC 62859, Requirements for coordinating safety and cybersecurity (ref. [71]).

1. C&I standards listed by the RP as referenced (ref. [30]) include:

* IAEA SSG-39, Design of instrumentation and control systems for nuclear power plants (ref. [24]).
* Licensing of safety critical software for nuclear reactors – Common position of international nuclear regulators (ref. [26]).
* NEA MDEP DICWG common positions on treatment of common cause failures, software tools, verification and validation, data communication, HDL-programmed devices, simplicity, industrial digital devices of limited functionality, cyber security, I&C architecture, automatic testing and spurious actuation (ref. [72]).
* IEC 61500, Data communication in systems performing category A functions (ref. [73]).

1. Another 45 supporting nuclear IEC standards are listed as referenced.
2. C&I standards and guidance listed by the RP as informative (ref. [30]) that I consider to contain significant relevant good practice include:

* IAEA SSR-2/1, Safety of nuclear power plants: Design (ref. [22]).
* SSG-30, Safety classification of structures, systems and components in nuclear power plants (ref. [23]).
* IEC TR 63084, Platform qualification for systems important to safety (ref. [74]).
* IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems (ref. [75]).
* IET code of practice – Cyber security and safety (ref. [27]).
* IET code of practice for electromagnetic resilience (ref. [76]).
* IAEA NP-T-3.27, Dependability assessment of software for safety instrumentation and control systems at nuclear power plants (ref. [77]).
* NUREG/CR-6303, Method for performing diversity and defence-in-depth analyses of reactor protection systems (ref. [78]).
* NUREG-CR-7007, Diversity strategies for nuclear power plant instrumentation and control systems (ref. [79]).

1. Additional guidance listed as informative includes 40 IAEA technical reports.
2. I consider the use of gradation in standards compliance through the categories of adopted, referenced and informative to be reasonable. Although the rationale for this prioritisation is sound, with level 2 IEC nuclear standards providing the primary benchmark for compliance, the following potential issues will need to be addressed as the standards are applied by the RP.
3. The documented intent of IAEA SSG-39 is to define the technical principles to be addressed in the design of nuclear C&I safety systems. In recognition of this, the IEC nuclear standards state that their aim is to provide detailed requirements on how these principles may be achieved. SSG-39 requirements use “should” even though they are above the IEC standard’s mandatory requirements that use “shall”.
4. Parts of some guidance that the RP lists only as informative provide key benchmarks for my Step 2 assessment (see section 2.1.3).
5. The RP distinguishes between product requirements, which the SMR design needs to meet, and process requirements, which determine the process for developing the design. Product requirements from adopted and referenced standards will be directly transferred to the RP’s requirements management system; but process requirements will not be. The RP’s stated basis for this distinction is that process requirements will already be covered in its existing development processes. However, C&I safety demonstration has a strong reliance on showing how the development process is commensurate with that defined in relevant good practice, which is likely to require more specifically documented traceability of the relevant standards’ process requirements.
6. The RP intends to create its own set of internal C&I standards that capture all relevant good practice from the documents listed in its selection report. The suitability of these internal standards and demonstration of their application will be part of my Step 3 assessment.
7. In summary, I am content that SAP ECS.3 (codes and standards) is met in principle for the current status of the C&I design. I have not found any significant relevant good practice to be missing from the standards and guidance the RP has identified. I plan to assess the RP’s internal standards to confirm that no relevant good practice is missed, especially for requirements that are not captured in the RP’s requirements management system (because they are categorised as process requirements) or belong to standards/guidance listed as informative.
   * 1. Categorisation and classification
8. ONR fault studies and severe accident analysis topic specialists led the assessment of the RP’s categorisation and classification method (ref. [31]) and have concluded that the method is largely consistent with relevant good practice defined in IAEA SSG-30 (ref. [23]) and NS-TAST-GD-094 (ref. [21]), but that appropriate demonstration of its application will be necessary in Step 3 (ref. [80]). I provided support to this assessment (ref. [81]) confirming that C&I aspects of the method meet relevant good practice defined in IEC 61226 (ref. [25]).
9. I consider that the most significant C&I systems, specifically the class 1 diverse protection system (DPS), the class 2 reactor protection system (RPS), the class 2 post-accident management system (PAMS), the class 3 severe accident management system (SAMS) and the class 3 reactor plant control and monitoring system (RPCMS), have been classified correctly according to the documentation submitted in Step 2. These systems are discussed in more detail in section ‎4.2.4.
10. I conclude that SAPs ECS.1 (safety categorisation) and ECS.2 (safety classification) are met in principle for the most significant systems at this stage of the design. Part of my assessment for all C&I systems sampled in Step 3, including those already listed, will be to confirm that the relevant safety functions are categorised correctly in line with their safety importance and that the systems and components implementing them have the necessary safety class.
    * 1. C&I architecture

**C&I systems overview**

1. The class 3 reactor plant control and monitoring system (RPCMS) includes the reactor plant control system (RPCS). The RPCS delivers duty functions during normal operating conditions to maintain control of the process parameters of the primary reactor systems and associated heat exchangers. During abnormal operating conditions, the RPCS delivers preventative functions designed to restore the primary reactor systems and associated heat exchangers to their normal operating conditions without actuating the reactor protection functions or other engineered safety features. The RPCS also controls the duty heating, ventilation and air conditioning (HVAC). The safety functions are all category C. The other constituent of the RPCMS is the reactor plant monitoring system (RPMS), which monitors non-safety critical parameters of the reactor to provide condition monitoring.
2. The class 2 reactor protection system (RPS) provides a secondary means of implementing all category A safety protection functions and a primary means of implementing category B protection functions. The RPS includes subsystems for processing output from neutron detectors, cutting power to the control rod drive mechanisms, prioritising actuation, monitoring and maintenance, and interfacing with operators in the main and supplementary control rooms (including panels, displays, alarms, manual protection actions and bypassing).
3. The class 1 diverse protection system (DPS) provides a diverse primary means of implementing category A safety protection functions. It includes diverse class 1 panels and displays for operators in the main and supplementary control rooms. The DPS also includes a class 2 DPS monitoring system (DPSMS), which monitors the DPS and displays this monitoring information in the control rooms.
4. The accident management system (AMS) provides monitoring for preventative and mitigative accident management. The AMS consists of the class 2 post-accident management system (PAMS) for design basis accidents and the class 3 severe accident management system (SAMS) for design extension conditions and severe accidents. The PAMS functional requirements and necessary safety classes are derived from IEC 63147 (ref. [82]) and associated application guidance (ref. [83]). SAMS is currently expected to only implement category C functions.
5. A novel aspect of the RP’s design is that the class 2 RPS will sometimes operate before the class 1 DPS, because the more complex RPS functions shutdown the plant in a way that facilitates resumed operation once the plant is in a restored condition. The less complex functionality of the DPS makes it more practicable to implement in a purely hardware-based system, with a consequent reduced safety demonstration burden for achieving class 1 reliability. ONR’s fault studies assessment (ref. [80]) concludes that this novel aspect of the operational philosophy aligns with SAP FA.7 (consequences), although its implications for the design and safety justification will be assessed further in Step 3.
6. I consider that the above set of C&I systems satisfies in principle SAP ESS.1 (provision of safety systems) and NS-TAST-GD-003 on safety systems (ref. [18]) for this stage of the design.

**Integrity targets**

1. The safety integrity targets for each system are set out in Table 1. This correlates with the ranges outlined in NS-TAST-GD-046 (ref. [20]), but 1E-3 probability of failure on demand (pfd) is beyond ONR’s initial expectation for class 2 computer based safety systems and hence will require stronger safety demonstrations (see ‎4.2.6). I conclude that the claims are appropriately defined and are in principle achievable, satisfying SAP ERL.1 (form of claims) for this stage of the design.

Table 1: System integrity targets

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | RPCS | RPS | DPS | PAMS | SAMS |
| Safety class | 3 | 2 | 1 | 2 | 3 |
| Probability of dangerous failure | 1E-1 per year or pfd | 1E-3 pfd | 1E-4 pfd | 1E-3 per year | 1E-1 per year or pfd |
| Spurious failures per year | 1E-1 | 1E-3 | 1E-3 to 1E‑5 | No target specified | 1E-1 |

**System independence**

1. Full independence (including against systematic failures) is required between systems providing different layers of defence-in-depth – that is between the RPCMS, the RPS/DPS and the SAMS. It is also required between the primary and secondary means of providing the same safety function, ie between the RPS and the DPS. This is to satisfy both the deterministic objective that these systems effectively compensate for each other’s failures, and the probabilistic assumption that the overall risk reduction provided by the combined systems for a fault is the product of their failure frequencies.
2. Design diversity is the principle means for achieving this system independence for systematic failures. The RP has identified these requirements for independence and plans to apply three diverse platforms, each using different technologies procured from different manufacturers.
3. The RP plans that the DPS platform will be hardwired, based on non-programmable hardwired technology. The DPS platform will also host the SAMS. The RP claims independence between the DPS and SAMS will be achieved by function and signal diversity.
4. The use of a hardwired class 1 diverse protection system reinforces up-to-date relevant good practice for nuclear power plants in the UK, illustrating the ongoing practicability of a hardwired C&I protection system to reduce risks ALARP and to achieve security by design (see ‎4.2.8).
5. The RP plans that the RPS platform will be complex programmable technology. The RP states diverse initiating parameters will be used between the RPS and DPS so far as is reasonably practicable. The RPS platform will also host PAMS, which is not required to be independent of the RPS.
6. The RPCMS platform will be a diverse complex programmable technology. This will also host other duty C&I systems such radioactive waste and fuel route (for which the design is currently less mature).
7. None of the platform technology solutions have been selected during Step 2.
8. The C&I engineering schedule (ref. [40]) provides a list of all safety functions implemented by C&I systems, including the system(s) it is allocated to, the initiation parameters and actuators. It provides a good indication of the current status of the design, providing clear visibility of assumptions and unresolved issues where independent parameters have not yet been determined.
9. The RP has produced a preliminary analysis (ref. [84]) of the diversity between the RPS and DPS using the method defined in NUREG/CR-7007 (ref. [79]) as example evidence for the safety demonstration. I consider this method to be relevant good practice and found the approach to be helpful, but noted that the scope will need expanding to include the full extent of the safety functions including sensors, actuators, essential support systems and operator actions (where applicable).
10. The RP has demonstrated awareness that communications between the C&I systems should not undermine independence. The high-level design shows one-way communication only from higher to lower safety class systems. This avoids a higher reliability requirement for a system being compromised by its responses to lower reliability data from another system. The RP has also stated it will consider the effect of these one-way signals on required independence of functions for the same fault sequence. I consider that this satisfies SAP ESS.20 (avoidance of connections to other systems), for this stage of the design.
11. Physical separation, barriers and civil structures will be needed to achieve necessary independence, particularly against internal hazards. The existing layout shows awareness of this requirement, which I will assess in more detail in Step 3. ONR’s assessment of independence in the presence of foreseeable internal hazards is carried out by internal hazards, which has concluded in Step 2 that the general layout for C&I is consistent with relevant good practice but barrier solutions, cable routing, location of the main control room and internal hazards within the interspace and containment block all require further analysis before the RP can demonstrate adequate management of hazard sources and their segregation (ref. [85]).
12. I consider that the high-level C&I system architecture, particularly the use of a hardwired non-programmable platform for the class 1 DPS, forms a good basis to meet SAPs EKP.3 (defence-in-depth), EDR.2 (redundancy, diversity and segregation), EDR.3 (common cause failure) and ESS.18 (failure independence). My further assessment of the justification that the required independence has been achieved will be a key feature in Step 3, including potential common cause failures between the DPS and SAMS due to the common hardwired platform.

**Redundancy and single failure criterion**

1. The C&I system redundancies are presented in Table 2. This has been driven by reliability requirements, and the single failure criterion where applicable.

Table 2: C&I system redundancies

|  |  |
| --- | --- |
| C&I system | Redundancy |
| DPS | 4 |
| RPS | 3 |
| PAMS | 3 |
| SAMS | 2 |
| RPCS | Duty and standby |
| RPMS | 1 |

1. The class 1 DPS has 4 redundancies to satisfy the single failure criterion, accounting for consequential loss of one redundancy from the initiating event and unavailability of one redundancy due to online maintenance. However, the 3-loop boiler design of the RR SMR limits to 3 redundancies the actuation of relevant DPS functions. The RP has stated that, in order to meet the single failure criterion, no online maintenance will occur for the necessary actuating components (ref. [80]). This meets the requirements of SAP EDR.4 (single failure criterion).
2. However, SAP FA.6 (fault sequences) expects the application of the single failure criterion to all design basis fault sequences (those with a frequency greater than 1E-7 per year). If any of these sequences are mitigated only by category B safety functions, with the class 2 RPS being the primary and only means, the RP will need to consider appropriate application of the single failure criterion to the RPS, which is not recognised currently in the RP’s C&I submissions (for example E3S chapter 7 issue 2, ref. [3]). The RP has acknowledged this in its response to fault studies regulatory query RQ-01085. Although currently the RPS is not the primary means of protection against any design basis fault sequences, relevant aspects of the fault analysis are not yet finalised, and this will be examined in partnership between fault studies and C&I in Step 3.
   * 1. C&I functional and property claims
3. The E3S case C&I chapter (ref. [3]) describes how the RP has derived control logic requirements for C&I systems for key reactor protection safety measures (scram, emergency core cooling and passive decay heat removal) from the fault schedule (ref. [86]) and recorded them in its requirements management database. The RP has also identified other functions likely to be required, including product requirements of adopted and reference standards (as discussed in para ‎61), and has documented these in the database as assumptions. The C&I engineering schedule (ref. [40]) provides a full list of these requirements and their allocation to C&I systems, to aid traceability and analysis. These requirements become C&I functional claims for each system.
4. The RP has derived non-functional requirements, which become C&I property claims, from its design principles and from adopted and referenced standards.
5. The RP’s requirements management database includes tools to document and present requirements hierarchy and traceability. However, these tools are not available to ONR, and the RP does not plan to provide these as part of GDA. Instead, submissions will include snapshots of the database presented as text documents containing spreadsheets.
6. I have reviewed an example showing the status of requirements in the database for the reactor island protection systems (ref. [39]). Not all requirements have been defined at this stage of the design and many are documented as needing further analysis. The submission provides visibility of the results of requirements derivation, but a later snapshot when this process has finished is likely to also need additional E3S case documentation to facilitate a convincing argument that the requirements are complete.
7. In summary, I consider that the RP has established and begun implementing an adequate framework to satisfy SAP ESS.2 (safety system specification). Demonstration of completeness of these requirements, and hence of the C&I functional and property claims, is discussed further in the next section.
   * 1. Safety demonstration

**Overall framework**

1. The RP’s intent is to provide a trail from claims through argument to evidence in its E3S case, with each chapter setting out the claims and referencing tier 2 and 3 evidence to support them (see ‎3.2). The RP initially indicated that all supporting claims relevant to the E3S case would be recorded as E3S requirements in its requirements management database, which would then be used to demonstrate traceability that every claim is met (with tier 2 and 3 documents providing supporting evidence). However, as discussed above, the traceability tools will not be available to all users of the E3S case, including ONR, and it is unclear how this trail will be demonstrated. For example, it is unclear how safety claims will be highlighted in this trail and be sufficiently supported by integrated arguments that link to the evidence, especially if the documentation does not specifically identify supporting claims beyond the E3S chapter.
2. ONR has raised a regulatory observation (RO) at the project level on the adequacy of E3S case arrangements. In an engagement to discuss this RO (ref. [87]), the RP stated that the trail from claim through argument to evidence will be documented in updates to system design descriptions (SDDs) and safety measure design descriptions (SMDDs), supported by tier 3 evidence.
3. I set out my current assessment position based on my understanding of the RP’s position, that for this trail to be sufficiently visible and complete the following conditions will be necessary:

* The CAE route map references all E3S requirements;
* All the E3S requirements show the full breadth of safety measures and systems they apply to, and
* The SMDDs and SDDs provide the argument for the full set of E3S requirements that apply to each of them, including consideration of design review documentation.

1. The RP agreed with this as a preliminary position during the meeting, but is still progressing its resolution of the regulatory observation and this has yet to be supported by any project documentation. It is uncertain that SMDDs and SDDs alone will provide sufficient coverage for all relevant supporting claims / E3S requirements. Unless the SMDDs and SDDs themselves contain lower level supporting claim structures, it is unclear how the trail from E3S requirements provided in the E3S chapter will include the supporting claims necessary to present the argument to the tier 3 evidence.

**C&I CAE framework**

1. I have reviewed the E3S case CAE route map (ref. [41]). Chapter 3 (safety objectives and design rules for SSCs) claims relate to high level design principles (categorisation/classification, dose limits, defence-in-depth, standards compliance, design basis analysis, examination, maintenance, inspection and test, and verification and validation) with no further detail on the properties necessary to achieve the design and how this will be demonstrated, other than very broad descriptions of tier 2 documents such as E3S design principles and requirements database transverse requirements. Likewise, the claims for chapters 6 (engineered safety features) and 7 (C&I) state that functional and non-functional requirements are correct and will be met, requirements are correctly assigned/allocated, and refer to categorisation/classification, verification and validation and examination, maintenance, inspection and test. Properties, key functional requirements, design features and methods are all implicitly allocated to tier 2 arguments/evidence.
2. Although this provides some indication of the RP’s safety demonstration approach, I consider that the route map is currently incomplete in its coverage of high-level claims for C&I and does not provide a clear indication of how those claims that do exist will be met.
3. The RP is in the process of developing a more rigorous, detailed and extensive CAE structure for C&I, in tandem with E3S case arrangements.
4. C&I E3S case submissions to date have not been clearly linked to claims, and the immature status of the current CAE structure would make this difficult. The RP has indicated its future intent is for its C&I E3S documentation to be much more clearly integrated with CAE, so for example it is clear what claim it is that any particular document provides evidence to support.
5. The RP stated at the E3S case RO engagement meeting that the latest C&I approach to CAE is considered relevant good practice and will be applied throughout the wider E3S case. It is unclear to what extent this is fully practicable and will be optimal for the requirements of each topic. From a C&I perspective, it will be important to ensure integration and coherence with the rest of the E3S case.
6. In summary, from a C&I perspective, the RP’s E3S case arrangements and implementation are not yet adequate to satisfy SAP SC.2 (safety case process outputs). The RP is currently taking actions in response to the relevant project-level regulatory observation and feedback during C&I level 4 meetings to address this shortfall. Its resolution will be part of my assessment for Step 3.

**Scope of C&I systems**

1. My future C&I assessment will need to consider every part of a system needed to carry out the safety function, including sensors, actuators, and operators where needed, for example for monitoring or in response to alarms. The scope of reactor C&I safety systems are limited by the RP to those parts of the overall system that are the responsibility of the RP’s C&I. Hence, for example, the RP considers the RPS to include its operator interface, displays and alarms, but not sensors or actuators (which are the responsibility of mechanical engineering). SDDs only provide details of the C&I system as defined by the RP. SMDDs provide full details of all required systems and components, but are only available for particular safety functions. The combined information has been sufficient for Step 2 but, in Step 3, the safety demonstration, including CAE, will need to be consistent and complete across both these document types.

**C&I safety demonstration planning**

1. In line with the relevant good practice defined in chapter 1.1 (safety demonstration) of the TF SCS common position for safety critical software (ref. [26]), the RP produced a reactor island C&I outline safety demonstration plan (ref. [45]), followed at the end of Step 2 by safety demonstration plans for the DPS (ref. [46]), RPS (ref. [47]) and smart devices (ref. [48]).
2. I assessed the outline plan, reviewed all three later plans and have assessed the smart devices plan in more detail. Since the RP has not yet selected the suppliers for any C&I systems, the specific techniques and methods for generating the necessary evidence have not yet been identified. However, the plans do show a good awareness of relevant good practice including ONR expectations documented in SAP ESS.27 and NS-TAST-GD-046 (ref. [20]).
3. NS-TAST-GD-046 (ref. [20]) states that the safety demonstration for a computer based safety system should consist of two independent legs: assessment of production excellence (PE) and independent confidence building measures (ICBMs). Any deficiencies found in the PE assessment should be compensated for by confirmatory measures, which complete the PE leg. The RP’s plans list assessment of production excellence (PE) as only as an independent confidence building measure (ICBM), making it unclear how PE will be demonstrated. In addition, confirmatory measures are listed as ICBMs rather than part of PE. However, in its response to regulatory query RQ-1234 (ref. [88]), the RP clarified that the PE demonstration will include compliance with adopted standards, subject to independent technical review, and will incorporate the process requirements from standards and other relevant good practice. Future plans will be revised to incorporate independent assessment of PE and compensating activities as part of the PE demonstration.
4. The RP currently plans that ICBMs will not include another fully independent review of PE (which is listed as an expectation in SAP ESS.27 and its supporting paragraph 424(a)(ii)). An appropriate set of ICBMs will vary significantly depending on supplier, system, technology and application context. Depending on the technology selected and degree of access to supplier development documentation, there may be opportunities for new ICBMs, not envisaged in the previous good practice that is consolidated in ESS.27 and NS-TAST-GD-046. Techniques that could add new contributions to the overall evidence base include for example metrics-based quality measurement and process improvement, and extensive convincing evidence of relevant operational dependability. It will only be possible for me to judge the adequacy of the ICBM set to be proposed when all the relevant information becomes available in Step 3.
5. The smart device safety plan states that production excellence will be assessed and demonstrated using IEC 62671 (ref. [60]) as the primary benchmark for compliance, rather than applying the CINIF Emphasis tool to demonstrate compliance against IEC 61508 (ref. [75]), which is UK relevant good practice. One reason for this is to make the overall safety demonstration more aligned to international practice. Emphasis may still be applied in particular situations, for example where assessments carried out by other licensees are available for reuse. There is a substantial gap between the requirements of IEC 61508 and IEC 62671 in the rigour of the software development process, which the RP intends to address through supplemental guidance for assessment. During Step 3, I will assess the adequacy and application of this supplementary material, which will include a case study smart device demonstration.
6. ONR’s electrical assessment (ref. [89]) has found that the RP intends to use smart devices within class 2 and 3 electrical systems. The RP states that its approach to use and qualification of smart devices will be managed by C&I. I will support the Step 3 electrical assessment in ensuring that this approach is appropriate and consistent with that applied for C&I safety systems.
7. In summary, safety demonstration plans are currently incomplete as they do not yet document the set of measures and techniques that will be applied to provide necessary evidence. But they do provide a good awareness of relevant good practice and present a credible initial framework for determining an adequate set. Taking account of the stated intentions of the RP for future work and revisions of safety demonstration plans, I consider the expectations of SAPs ESS.11 (demonstration of adequacy) and ESS.27 (computer-based safety systems) are met for the current design status.
   * 1. Essential services
8. The RP’s summary of essential services for supporting reactor island C&I safety systems (ref. [42]) identifies heating, ventilation and air-conditioning (HVAC) systems and electrical power supply as the only two essential services for reactor C&I safety systems.
9. Support functions of essential services are categorised to match the safety function that they support, although this is relaxed by one step (eg a reduction from category A to B) if there is opportunity for repair or replacement of the failed support function before the safety function fails.
10. The HVAC that supports the RPS and DPS will have the same requirements for diversity, redundancy and reliability as the systems they support. Hence the class 1 DPS will be supported by class 1 HVAC, and the class 2 RPS by class 2 HVAC. The four divisions of the DPS will each by supported by four separate HVAC (and likewise for the three divisions of the RPS). Failure or spurious operation is required not to compromise the independence between redundant divisions of safety system and between systems at different levels of defence-in-depth. A separate class 3 HVAC will provide duty HVAC services for all C&I safety systems on the reactor island. The DPS and RPS will independently monitor their own environments and trigger their respective class 1 and 2 HVAC when required.
11. ONR assessment of the HVAC design (ref. [90]) is led by mechanical engineering. This assessment concludes that the HVAC design is not yet sufficiently mature to judge whether or not the requirements will be met. I will continue liaising in my assessment with the mechanical engineering inspector to facilitate this judgement during Step 3.
12. The electrical power systems are the subject of a dedicated electrical assessment (ref. [89]), which considers their adequacy to support the required C&I safety functions.
13. The use of four redundant divisions of class 1 batteries to support the DPS, and three redundant divisions of class 2 uninterruptible power supplies to support the RPS, is consistent with the C&I architecture. Independence between divisions and between the RPS and DPS is a documented requirement, but the design at this stage does not show how this will be achieved. ONR’s Step 3 electrical assessment plans to consider the RP’s demonstration of independence.
14. The electrical assessment concludes that the proposed basic electrical system architecture, including support to reactor C&I safety systems, is consistent with relevant good practice, providing a robust defence-in-depth capability.
15. Future revisions of the essential services summary (ref. [42]) will include the results of the RP’s determination of the adequacy of the design for C&I requirements.
16. In summary, I consider that SAP EES.1 (provision of essential services) for reactor C&I safety systems is met in terms of documented requirements and architecture to the design level attained during Step 2. ONR will continue to assess the design adequacy in Step 3 as the detail progresses, with electrical leading for the electrical power supply and mechanical engineering leading for the HVAC.
    * 1. Cyber security for safety
17. ONR’s assessment of cyber security is led by cyber security and information assurance (CS&IA) under the security lead. I have supported this assessment to help confirm the adequacy of cyber security arrangements necessary to ensure dependable operation of C&I safety systems.

**Secure by design**

1. The RP has developed a secure by design method (ref. [43]) to eliminate or reduce cyber security risks through early design decisions. The RP tested the method in an early analysis of its application to the DPS (ref. [91]) and produced a summary report (ref. [92]) of the current status.
2. The RP refers to its decision to implement the DPS in non-programmable hardware technology, to provide immunity from cyber attack, as an outcome of its secure by design method. I agree that this single design decision considerably reduces the overall risk of unacceptable radiological consequences through cyber security compromise of the overall C&I reactor protection. The provision of a non-programmable DPS is up-to-date relevant good practice for cyber security resilience in the C&I protection architecture for nuclear power plants in the UK, illustrating the ongoing practicability of a hardwired C&I protection system to achieve the required defence-in-depth and cyber security resilience.
3. The secure by design analysis and summary report also refers to the cyber security risk assessment of the DPS as complete (albeit to be repeated), without any discussion or learning from the limitations of this assessment discussed later in this section. I consider this to be a missed opportunity for process improvement.
4. Overall, ONR’s security assessment (ref. [93]) concludes that the secure by design method and its application adequately demonstrates the foundations for achieving success. I will continue to support the security assessment in the application of security by design to detailed design decisions affecting the safety objectives of C&I in Step 3.

**Risk assessment**

1. The RP’s cyber security risk assessment method (ref. [44]) has been subject to revision since its first submission, taking account of feedback from ONR and internal review. Its process is aligned to IEC 62443-3-2 (ref. [94]), it incorporates security degree requirements from IEC 62645 (ref. [70]), techniques from the MITRE ATT&CK framework (ref. [95]) and control sets using requirements from IEC 62645, IEC 63096 (ref. [96]) and IEC 62443-3-3 (ref. [97]).
2. I advised the RP that the proposed method for assessing multiple systems does not provide a means for determining whether safety claims for independence between C&I safety systems (see ‎4.2.4) still hold with respect to foreseeable cyber security compromise. The revised submission still contains this shortfall although the RP has shown an understanding of the requirement in its response to regulatory query RQ-01215 (ref. [88]), and committed to meet it in a future update of the method. This will be important, in Step 3, for ensuring the validity of the C&I safety demonstration and determining security design aspects such as zoning that sustain independence.
3. Security degrees for computer based systems important to safety are used to determine the grading of necessary security controls. The security degree for each system is assigned based on whether or not the system has an impact on safety when manipulated maliciously, with S1 aligned with the consequences of failure of functions of safety category A, S2 with safety category B, and S3 with systems that cannot have an impact. I have not yet gained sufficient confidence that this application of systems, function categories and safety impact is fully understood by the RP. In response to regulatory query RQ-01053 (ref. [88]), the RP clarified that systems with consequences of failure equivalent to safety category C will be assigned security degree S3. It is possible that this labelling of category C as being of no safety impact could have negative consequences in the coherence of cyber security claims for safety systems. Likewise it is unclear how the mapping between system class and safety function category consequence will be worked out in practice in these security degree assignments. I will assess this aspect during Step 3 in the context of the method’s practical application.
4. The RP carried out a trial cyber security risk assessment for the RPS and the DPS (ref. [49]). The risk assessment refers to the DPS as a “secondary layer of protection within the defence-in-depth argument” (missing that it is the primary means for category A functions) and incorrectly concluded a low risk ranking for the DPSMS based on the erroneous assertion that because it is a monitoring system it has no safety significance (the DPSMS is class 2 because its functions have a key role in supporting the DPS). The assessment for the RPS assumed that a cyber attack could only affect one RPS division, with no credible justification. In terms of testing the rigour of the risk assessment method for C&I safety systems and the arrangements for co-ordination with the RP’s C&I safety expertise, the trial has revealed significant shortfalls in the initial approach. Risk assessments for the DPS and RPS will be updated during Step 3. The RP has committed to providing full justifications in its assessments and recognises that the safety class of a C&I system is a key indicator of its safety importance to be respected in the assessment. Co-ordination between cyber security and safety is discussed below.
5. The ONR security assessment (ref. [93]) accounts for our joint findings and concludes that the RP has sufficiently met ONR expectations for cyber security risk assessment, considering the RP’s commitments to further develop its methods and processes. I will liaise closely with security and CS&IA in Step 3 to support the CS&IA objectives, including resolving the safety issues identified above.

**Co-ordination with safety**

1. I have led ONR’s assessment on ensuring effective co-ordination of safety and cyber security activities and development lifecycles. The RP has developed a set of governing principles, utilising the IET code of practice on cyber security and safety (ref. [27]), and carried out a gap analysis for these principles against its current arrangements (ref. [98]). This includes a commitment to define interaction points between safety and cyber security processes and specify supporting analysis techniques. I consider the identification of requirements a positive step, progressing relevant good practice for co-ordination of safety and cyber security, and will be assessing the RP’s plan for meeting these requirements in Step 3.

**Development process and product assurance**

1. In its response to regulatory query RQ-01236 (ref. [88]), the RP acknowledges the need to define methods and techniques to find and resolve cyber security vulnerabilities introduced during the software development of C&I systems important to safety. In line with the recommendations of ONR security TAG CNS-TAST-GD-7.3 on protection of nuclear technology and operations (ref. [99]), this will mirror the ESS.27 framework of production excellence and independent confidence building measures. The methods and techniques to be applied will be detailed in future revisions of safety demonstration plans (retitled safety and security plans), led by C&I. I will assess these in Step 3 in consultation with CS&IA.
   * 1. ALARP
2. At the current stage of the design, it is only possible to consider whether risks have been reduced to as low as is reasonably practicable (ALARP) in terms of high level architecture, design principles and documented requirements.
3. I consider that the RP’s approach to developing its C&I systems is broadly consistent with the expectations of UK/international relevant good practice. The RP has identified an appropriate set of reference and informative standards and guidance, and to date its application of these benchmarks has been in line with expectations. In line with the guidance in NS-TAST-GD-005 (ref. [19]), this is a key component of an ALARP demonstration.
4. As the design increases in detail, my Step 3 assessment will sample the claims, arguments and evidence necessary to underpin a comprehensive safety demonstration that the C&I has been designed to reduce risks to ALARP.

# Conclusions

* 1. Conclusions

1. This report presents my Step 2 C&I assessment for the GDA of the Rolls-Royce SMR design. The focus of my assessment in this step was the fundamental adequacy of the design and safety case. I have assessed the tier 1 E3S chapters and relevant supporting documentation provided by Rolls-Royce SMR Limited to form my judgements. I found the supporting documentation to be consistent with the E3S chapter. I targeted my assessment, in accordance with my assessment plan (ref. [11]), at the content most relevant to C&I against the expectations of ONR’s SAPs, TAGs and other standards and guidance which ONR regards as relevant good practice.
2. Based upon my assessment, I have concluded the following. I plan to follow up all of these aspects in my Step 3 assessment.

* The RP’s design principles are complete at a high level and demonstrate good alignment with ONR’s expectations for overall design goals. It is unclear at this stage how the principles will be carried through in the E3S case to provide a clear trail from claims through arguments to evidence.
* The RP’s documented set of C&I reference standards and guidance provides an appropriate benchmark for relevant good practice, with reasonable gradation in how compliance will be demonstrated. The set of internal C&I standards, still to be created by the RP, will need to capture all relevant good practice for both product and process requirements, some of which are contained in standards and guidance the RP has labelled as only informative.
* The RP’s method for categorisation and classification is largely consistent with relevant good practice and has been applied appropriately for the reactor C&I safety systems based on the design information currently available.
* The RP has identified an appropriate set of reactor C&I safety systems based on the current design information, with system integrity targets consistent with their classes, although the 1E-3 pfd/per year targets for the class 2 systems will require a stronger safety demonstration than the default for class 2. The high level architecture has the potential to achieve the necessary system independence. The single failure criterion will apply to the class 2 RPS if it is the primary and only means for implementing any functions mitigating design basis fault sequences. Although this is not the case in the current design, relevant aspects of the fault analysis are not yet finalised.
* The use of a hardwired class 1 diverse protection system has strong potential to provide an effective means of achieving independence from the class 2 reactor protection system for defence-in-depth. It reinforces up-to-date relevant good practice for nuclear power plants in the UK, illustrating the ongoing practicability of a hardwired C&I protection system to reduce risks ALARP.
* The RP has established and begun implementing an adequate framework for C&I functional and property claims, but demonstration of completeness requires further development of the RP’s E3S case arrangements.
* The RP’s E3S case arrangements and application of CAE is the subject of a project-level ONR regulatory observation. From a C&I perspective, the RP’s arrangements and implementation do not satisfy ONR expectations and will need to be addressed to enable the RP to provide a coherent C&I safety demonstration.
* Safety demonstration plans for C&I systems, which identify the set of PE and ICBM methods and techniques required to generate the evidence to support claims for each system, are incomplete but provide good awareness of relevant good practice and present a credible initial framework for determining an adequate set.
* Requirements and indicative high-level architecture for essential systems for C&I, namely electrical power supplies and HVAC, meet ONR expectations for C&I at this stage of the design.
* The RP’s secure by design method and it’s application indicates the foundations for achieving success of this objective. The use of a hardwired class 1 diverse protection system is an exemplar application of security by design, considerably reducing the overall risk of any cyber attack leading to unacceptable radiological consequences.
* The RP has sufficiently met ONR expectations for cyber security risk assessment, accounting for a commitment to develop a method for assessing the validity of independence claims for multiple systems considering foreseeable cyber security compromise. In determining appropriate controls, the RP’s method for assigning security degrees is potentially inconsistent in its application of the concepts of systems, function categories and no safety impact for category C functions. The suitability of the approach will need demonstrating through examples of practical application.
* The RP’s principles for the co-ordination of safety and cyber security activities and development lifecycles progresses relevant good practice and provides a good basis for developing its plan to meet these requirements. This will include developing combined C&I system safety and security demonstration plans to include PE and ICBM methods and techniques for finding and resolving cyber security vulnerabilities introduced during the software development of C&I systems important to safety.
* The RP’s development of its C&I systems is broadly consistent with the expectations of UK and international relevant good practice, which provides a sound basis to reduce risks to ALARP.

1. I raised no regulatory observations or regulatory issues during my assessment.
2. Overall, based on my assessment to date, and subject to the provision and assessment of suitable and sufficient supporting evidence, I have not identified any fundamental safety shortfalls that could prevent ONR permissioning the construction of a power station based on the generic Rolls-Royce SMR design.
   1. Recommendations
3. My recommendations are as follows:

* Recommendation 1: ONR should consider the outcomes from my assessment as part of the decision to progress to Step 3 of GDA for the generic Rolls-Royce SMR design.

References

|  |  |
| --- | --- |
| [1] | Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 1: Introduction, SMR0004294, Issue 3, May 2024. (Record ref. ONRW-2019369590-9881). |
| [2] | Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs, SMR0004589, Issue 3, May 2024. |
| [3] | Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 7: Instrumentation and Control, SMR0003929, Issue 3, May 2024. (Record ref. ONRW-2019369590-9887). |
| [4] | Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 24: ALARP Summary, SMR0004487, Issue 3, May 2024. (Record ref. ONRW-2019369590-9914). |
| [5] | Rolls-Royce SMR Limited, Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 32: Generic Security Report, SMR0004682, Issue 3, May 2024. (Record ref. ONRW-2019369590-9905). |
| [6] | ONR, Guidance on Mechanics of Assessment, NS-TAST-GD-096, Issue 1.2, December 2022. www.onr.org.uk/media/documents/guidance/ns-tast-gd-096.docx. |
| [7] | ONR, Safety Assessment Principles for Nuclear Facilities (SAPs), 2014 Edition, Revision 1, January 2020. www.onr.org.uk/media/pobf24xm/saps2014.pdf. |
| [8] | ONR, Technical Assessment Guides. www.onr.org.uk/publications/regulatory-guidance/regulatory-assessment-and-permissioning/technical-assessment-guides-tags/nuclear-safety-tags/technical-assessment-guides-tags-nuclear-safety-full-list/. |
| [9] | ONR, Guidance on the production of reports for permissioning and assessment, NS-TAST-GD-108, Issue 1, December 2022. (Record ref 2022/71935). |
| [10] | ONR, New Nuclear Power Plants: Generic Design Assessment Guidance to Requesting Parties, ONR-GDA-GD-006, Revision 0, October 2019. www.onr.org.uk/media/pylbvfnz/onr-gda-gd-006.pdf. |
| [11] | ONR, Step 2 control and instrumentation assessment plan for the generic design assessment of the Rolls-Royce SMR, ONR-GDA-AP-22-010, Issue 1, February 2023. (Record ref 2022/68797). |
| [12] | ONR, Generic Design Assessment of the Rolls-Royce SMR - Step 2 summary, ONRW-2019369590-8980, Issue No. 1, July 2024. (Record ref. ONRW-2019369590-8980). |
| [13] | Rolls-Royce SMR Limited, Rolls-Royce SMR Generic Design Assessment Scope, SMR0002183, Issue 2, January 2023. (Record ref. ONRW-2019369590-8058). |
| [14] | IAEA, Safety standards. www.iaea.org. |
| [15] | IAEA, Nuclear security series. www.iaea.org. |
| [16] | WENRA, Safety reference levels for existing reactors 2020. February 2021. WENRA. www.wenra.eu. |
| [17] | WENRA, WENRA safety objectives for new nuclear power plants and WENRA report on safety of new NPP designs - RHWG position on need for revision. September 2020. www.wenra.eu. |
| [18] | ONR, Safety systems, NS-TAST-GD-003, Issue 9.2, September 2022. www.onr.org.uk/media/documents/guidance/ns-tast-gd-003.docx. |
| [19] | ONR, Guidance on the demonstration of ALARP, NS-TAST-GD-005, Revision 11.2, June 2023. www.onr.org.uk/media/documents/guidance/ns-tast-gd-005.docx. |
| [20] | ONR, Computer based safety systems, NS-TAST-GD-046, Issue 7, December 2023. www.onr.org.uk/media/documents/guidance/ns-tast-gd-046.docx. |
| [21] | ONR, Categorisation of safety functions and classification of structures, systems and components, NS-TAST-GD-094, Revision 2, July 2019. www.onr.org.uk/media/documents/guidance/ns-tast-gd-094.pdf. |
| [22] | IAEA, Safety of nuclear power plants: Design, specific safety requirements no SSR-2/1, 2016. www.iaea.org. |
| [23] | IAEA, Safety classification of structures, systems and components in nuclear power plants, Specific safety guide no SSG-30, 2014. www.iaea.org. |
| [24] | IAEA, Design of instrumentation and control systems for nuclear power plants, specific safety guide no SSG-39, 2016. www.iaea.org. |
| [25] | IEC, Nuclear power plants - Instrumentation, control and electrical power systems important to safety - Categorisation of functions and classification of systems, IEC 61226, 2020. www.iec.ch. |
| [26] | TF SCS, Licensing of safety critical software for nuclear reactors - Common position of international nuclear regulators and authorised technical support organisations, Revision 2022. www.onr.org.uk/software.pdf. |
| [27] | IET, Code of practice - Cyber security and safety, 2021. www.theiet.org. |
| [28] | IAEA, Format and content of the safety analysis report for nuclear power plants, specific safety guide no. SSG-61, September 2021. www.iaea.org. |
| [29] | Rolls-Royce SMR Limited, Environment, safety, security and safeguards design principles, SMR0001603, Issue 1, August 2022. (Record ref. ONRW-2019369590-7775). |
| [30] | Rolls-Royce SMR Limited, C&I codes and standards selection report, SMR0004272, Issue 3, January 2024. (Record ref. ONRW-2019369590-7021). |
| [31] | Rolls-Royce SMR Limited, UK SMR environment, safefy, security and safeguards categorisation and classification method, EDNS01000887611, Issue 2, August 2021. (Record ref. 2022/51247). |
| [32] | Rolls-Royce SMR Limited, System design description - Reactor island control and protection systems [JY], SMR0007556, Issue 1, September 2023. (Record ref. ONRW-2019369590-4504). |
| [33] | Rolls-Royce SMR Limited, System design description for the reactor protection system [JRA], SMR0007347, Issue 1, October 2023. (Record ref. ONRW-2019369590-4869). |
| [34] | Rolls-Royce SMR Limited, System design description for the diverse protection system [JQA], SMR0007690, Issue 1, October 2023. (Record ref. ONRW-2019369590-4870). |
| [35] | Rolls-Royce SMR Limited, Scram safety measure design description, SMR0000639, Issue 2, October 2023. (Record ref. ONRW-2019369590-4931). |
| [36] | Rolls-Royce SMR Limited, Safety measure design description for emergency core cooling, SMR0000911, Issue 2, October 2023. (Record ref. ONRW-2019369590-4928). |
| [37] | Rolls-Royce SMR Limited, Safety measure design description for passive decay heat removal, SMR0000624, Issue 2, October 2023. (Record ref. ONRW-2019369590-4944). |
| [38] | Rolls-Royce SMR Limited, Safety measure design description for the alternative shutdown function [JD02], SMR0000638, Issue 2. December 2023. (Record ref. ONRW-2019369590-6062). |
| [39] | Rolls-Royce SMR Limited, Reactor island control and instrumentation - Requirements specification, SMR0000563, Issue 2, October 2023. (Record ref. ONRW-2019369590-4680). |
| [40] | Rolls-Royce SMR Limited, C&I engineering schedule, SMR0000510, Issue 2, June 2023. (Record ref. ONRW-2019369590-3365). |
| [41] | Rolls-Royce SMR Limited, E3S case route map, SMR0002155, Issue 3, November 2023. (Record ref. ONRW-2019369590-8059). |
| [42] | Rolls-Royce SMR Limited, Control and instrumentation: Support services summary, SMR0004778, Issue 1, November 2023. (Record ref. ONRW-2019369590-5432). |
| [43] | Rolls-Royce SMR Limited, Secure by design methodology, SMR0005789, Issue 1, May 2023. (Record ref. ONRW-2019369590-2870). |
| [44] | Rolls-Royce SMR Limited, Cyber security risk assessment methodology, SMR0006431, Issue 2, October 2023. (Record ref. ONRW-2019369590-4862). |
| [45] | Rolls-Royce SMR Limited, Reactor island C&I outline safety plan, SMR0008351, Issue 1, October 2023. (Record ref. ONRW-2019369590-4821). |
| [46] | Rolls-Royce SMR Limited, Safety plan for the diverse protection system [JQA], SMR0009252, Issue 1, January 2024. (Record ref. ONRW-2019369590-6603). |
| [47] | Rolls-Royce SMR Limited, Safety plan for the reactor protection system [JRA], SMR0008216, Issue 1, January 2024. (Record ref. ONRW-2019369590-6604). |
| [48] | Rolls-Royce SMR Limited, Smart device safety plan, SMR0006029, Issue 1, January 2024. (Record ref. ONRW-2019369590-6605). |
| [49] | Rolls-Royce SMR Limited, Cyber security risk analysis trial, SMR0008887, Issue 1, November 2023. (Record ref. ONRW-2019369590-5391). |
| [50] | Rolls-Royce SMR Limited, Rolls-Royce SMR – GDA Design Reference Report, SMR0009043, Issue 2, April 2024. (Record ref. ONRW-2019369590-8872). |
| [51] | IEC, Nuclear power plants - Instrumentation and control important to safety - General requirements for systems, IEC 61513, 2011. www.iec.ch. |
| [52] | BSI, Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions, BS EN 60880:2009 incorporating corrigendum June 2015. bsol.bsigroup.com. |
| [53] | IEC, Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category B or C functions, IEC 62138, 2018. www.iec.ch. |
| [54] | IEC, Nuclear power plants - Instrumentation and control important to safety - Hardware design requirements for computer-based systems, IEC 60987, 2021. www.iec.ch. |
| [55] | IEC, Nuclear power plants - Instrumentation and control important to safety - Development of HDL-programmed integrated circuits for systems performing category A fucnctions, IEC 62566, 2012. www.iec.ch. |
| [56] | IEC, Nuclear power plants - Instrumentation and control important to safety - Development of HDL-programmed integrated circuits - Part 2: HDL-programmed integrated circuits for systems performing category B or C functions, IEC 62566-2, 2020. www.iec.ch. |
| [57] | IEC, Nuclear power plants - Instrumentation and control systems important to safety - Requirements for coping with common cause failure, IEC 62340, 2007. www.iec.ch. |
| [58] | IEC, Nuclear power plants - Instrumentation, control and electrical systems important to safety - Separation, IEC 60709, 2018. www.iec.ch. |
| [59] | IEC, Nuclear power plants - Instrumentation and control systems important to safety - Management of ageing, IEC 62342, 2007. www.iec.ch. |
| [60] | IEC, Nuclear power plants - Instrumentation and control important to safety - Selection and use of industrial digital devices of limited functionality, IEC 62671, 2013. www.iec.ch. |
| [61] | IEC, Nuclear facilities - Electrical equipment important to safety - Qualification, IEC 60780-323, 2016. www.iec.ch. |
| [62] | IEC, Nuclear facilities - Equipment important to safety - Seismic qualification, IEC/IEEE 60980-344, 2020. www.iec.ch. |
| [63] | IEC, Nuclear power plants - Control rooms - Design, IEC 60964, 2019. www.iec.ch. |
| [64] | IEC, Electromagnetic compatibility - Testing and measurement techniques - Overview of 61000-4 series, IEC TR 61000-4-1, 2016. www.iec.ch. |
| [65] | IEC, Electromagnetic compatibility - Testing and measurement techniques - Electrostatic discharge immunity test, IEC 61000-4-2, 2008. www.iec.ch. |
| [66] | IEC, Electromagnetic compatibility - Testing and measurement techniques - Radiated, radio-frequency, electromagnetic field immunity test, IEC 61000-4-3, 2020. www.iec.ch. |
| [67] | IEC, Electromagnetic immunity - Testing and measurement techniques - Electrical fast transient/burst immunity test, IEC 61000-4-4, 2012. www.iec.ch. |
| [68] | IEC, Electromagnetic compatibility - Testing and measurement techniques - Surge immunity test, IEC 61000-4-5:2014, incorporating amendment 1:2017. www.iec.ch. |
| [69] | IEC, Electromagnetic compatibility - Testing and measurement techniques - Immunity to conducted disturbances induced by radio-frequency fields, IEC 61000-4-6, 2023. www.iec.ch. |
| [70] | IEC, Nuclear power plants - Instrumentation, control and electrical power systems - Cybersecurity requirements, IEC 62645, 2019. www.iec.ch. |
| [71] | IEC, Nuclear power plants - Instrumentation and control systems - Requirements for coordinating safety and cybersecurity, IEC 62859:2016 incorporating amendment 1:2019. www.iec.ch. |
| [72] | NEA, MDEP digital instrumentation and control working group common positions. www.oecd-nea.org. |
| [73] | IEC, Nucear power plants- Instrumentation and control systems important to safety - Data communication in systems performing category A functions, IEC 61500, 2018. www.iec.ch. |
| [74] | IEC, Nuclear power plants - Instrumentation and control important to safety - Platform qualification for systems important to safety, IEC TR 63084, 2017. www.iec.ch. |
| [75] | IEC, Functional safety of electrical/electronic/programmable electronic safety-related systems, IEC 61508, 2010. www.iec.ch. |
| [76] | IET, Code of practice for electromagnetic resilience, 2017. www.theiet.org. |
| [77] | IAEA, Dependability assessment of software for safety instrumentation and control systems at nuclear power plants, Nuclear energy series no NP-T-3.27, 2018. www.iaea.org. |
| [78] | US NRC, Method for performing diversity and defence-in-depth analyses of reactor protection systems, NUREG/CR-6303, 1994. www.nrc.gov. |
| [79] | US NRC, Diversity strategies for nuclear power plant instrumentation and control systems, NUREG/CR-7007, 2008. www.nrc.gov. |
| [80] | ONR, Generic Design Assessment of the Rolls-Royce SMR - Step 2 assessment of Fault Studies, ONRW-2126615823-2793, Issue No. 1, June 2024. (Record ref. ONRW-2126615823-2793). |
| [81] | ONR, Contact record: Rolls Royce SMR GDA - Level 4 fault studies cat & class method - 15 June 2023, ONR-NR-CR-23-117. (Record ref ONRW-2019369590-3082). |
| [82] | IEC, Criteria for accident monitoring instrumentation for nuclear power generating stations, IEC 63147, 2017. www.iec.ch. |
| [83] | IEC, Nuclear power plants - Instrumentation, control and electrical power systems - Guidance for the application of IEC 63147 in the IAEA / IEC framework, PD IEC/TR 63123, 2017. www.iec.ch. |
| [84] | Rolls-Royce SMR Limited, C&I substantation of achievability of diversity requirements, SMR0008449, Issue 1, October 2023. (Record ref. ONRW-2019369590-4871). |
| [85] | ONR, Generic Design Assessment of the Rolls-Royce SMR - Step 2 assessment of Internal Hazards, ONRW-2126615823-3464, Issue No. 1, June 2024. (Record ref. ONRW-2126615823-3464). |
| [86] | Rolls-Royce SMR Limited, Rolls-Royce SMR fault schedule (version 7), SMR0004444, Issue 3, January 2024. (Record ref. ONRW-2019369590-7004). |
| [87] | ONR, Level 4 RO-001 intervention - Testing the adequacy and implementation of the arrangements developed in response to RO-RRSMR-001 (development of the generic E3S case) - 5 and 12 March 2024, ONR-NR-CR-23-704. (Record ref ONRW-2019369590-8522). |
| [88] | ONR, Schedule of Step 2 regulatory queries, April 2024. (Record ref ONRW-2019369590-9071). |
| [89] | ONR, Generic Design Assessment of the Rolls-Royce SMR - Step 2 assessment of Electrical Engineering, ONRW-2126615823-3090, Issue No. 1, June 2024. (Record ref. ONRW-2126615823-3090). |
| [90] | ONR, Generic Design Assessment of the Rolls-Royce SMR - Step 2 assessment of Mechanical Engineering, ONRW-2126615823-3642, Issue No. 1, June 2024. (Record ref. ONRW-2126615823-3642). |
| [91] | Rolls-Royce SMR Limited, Secure by design analysis, SMR0009049, Issue 1, November 2023. (Record ref. ONRW-2019369590-4928). |
| [92] | Rolls-Royce SMR Limited, Secure by design report, SMR0009697, Issue 2, February 2024. (Record ref. ONRW-2019369590-6710). |
| [93] | ONR, Generic Design Assessment of the Rolls-Royce SMR - Step 2 assessment of Security, ONRW-2126615823-3520, Issue No. 1, June 2024. (Record ref. ONRW-2126615823-3520). |
| [94] | IEC, Security for industrial automation and control systems - Security risk assessment for system design, IEC 62443-3-2, 2020. www.iec.ch. |
| [95] | MITRE Corporation, ICS Matrix v14.0. attack.mitre.org/versions/v14/matrices/ics/. |
| [96] | IEC, Nuclear power plants - Instrumentation, control and electrical power systems - Security controls, IEC 63096, 2020. www.iec.ch. |
| [97] | IEC, Industrial communication networks - Network and system security - System security requirements and security levels, IEC 62443-3-3, 2013. www.iec.ch. |
| [98] | Rolls-Royce SMR Limited, C&I safety and cyber security integration strategy, SMR0004666, Issue 2, January 2024. (Record ref. ONRW-2019369590-7020). |
| [99] | ONR, Protection of nuclear technology and operations, CNS-TAST-GD-7.3, Issue 2, March 2022. (Record ref. 2022/6881). |

# Appendix 1 – Relevant SAPs considered during the assessment

|  |  |
| --- | --- |
| SAP No | SAP Title |
| SC.2 | Safety cases – Safety case process outputs |
| EKP.3 | Defence-in-depth |
| ECS.1 | Safety classification and standards – Safety categorisation |
| ECS.2 | Safety classification and standards – Safety classification of SSCs |
| ECS.3 | Safety classification and standards – Codes and standards |
| EDR.2 | Design for reliability – Redundancy, diversity and segregation |
| EDR.3 | Design for reliability – Common cause failure |
| EDR.4 | Design for reliability – Single failure criterion |
| ERL.1 | Reliability claims – Form of claims |
| ESS.1 | Safety systems – Provision of safety systems |
| ESS.2 | Safety systems – Safety system specification |
| ESS.11 | Safety systems – Demonstration of adequacy |
| ESS.18 | Safety systems – Failure independence |
| ESS.20 | Safety systems – Avoidance of connections to other systems |
| ESS.27 | Safety systems – Computer based safety systems |
| EES.1 | Essential services – Provision |
| FA.6 | Fault analysis – Fault sequences |
| FA.7 | Fault analysis – Consequences |