



SMR

© Rolls-Royce SMR Ltd, 2024, all rights reserved – copying or distribution without permission is not permitted.

# **Environment, Safety, Security, and Safeguards Case Version 2, Tier 1, Chapter 7: Instrumentation and Control**





## Record of Change

---

Date	Revision Number	Status	Reason for Change
March 2023	1	Issue	First issue of E3S Case
March 2024	2	Issue	It incorporates revisions and new design developments of the Instrumentation and Control based on Reference Design 7, aligned to Design Reference Point 1, including additional designs details and developments on systems included in the first issue.
May 2024	3	Issue	<p>Updated to correct revision history status at Issue 2. Chapter changes include:</p> <ul style="list-style-type: none"><li>• Additional descriptions of essential support services added to section 7.8</li><li>• Additional detail within conclusion section for how arguments and evidence presented meet the generic E3S objective</li></ul> <p>Also minor template/editorial updates for overall E3S Case consistency.</p>



## Executive Summary

Chapter 7 of the generic Environment, Safety, Security, and Safeguards (E3S) Case presents the Control and Instrumentation (C&I) of the Rolls-Royce Small Modular Reactor (RR SMR).

The chapter outlines the arguments and evidence to underpin the high-level claim that the RR SMR C&I systems are conservatively designed and verified to deliver E3S functions through-life, in accordance with the E3S design principles, to reduce risks to as low as reasonably practicable (ALARP), apply best available techniques (BAT) and ensure secure by design and safeguards by design.

The scope of chapter 7 covers all C&I systems. This revision, at Version 2 of the generic E3S Case, focuses on the Reactor Island Control and Protection System [JY], which includes the Reactor Protection System (RPS) [JRA], Diverse Protection System (DPS) [JQA], Accident Management System (AMS) [JRQ], and Reactor Plant Control and Monitoring System (RPCMS) [JS], with a brief summary of the other systems.

For each system, the safety functions to be delivered by each SSC are presented, with the assignment of safety categorised functional requirements to achieve them. Non-functional system requirements derived from the E3S design principles are described. The design definition presented for each system is developed based on relevant good practice (RGP) and operating experience (OPEX), with design to codes and standards according to the safety classification, and down-selection of options in accordance with criteria to ensure risks are reduced to ALARP, apply BAT, and are secure by design and safeguards by design. This provides confidence that claims can be met when the full suite of arguments and evidence is developed. No functional requirements for environment, security and safeguards are identified for the C&I SSCs.

Version 2 of the generic E3S Case is developed in support of the reference design 7 (RD7), corresponding to design reference point 1 (DRP1) for the generic design assessment (GDA). Further arguments and evidence are to be developed to underpin the top-level claim, including development of a complete set of E3S requirements and their associated verification and validation activities.



# Contents

---

	Page No
<b>7.0 Introduction to Chapter</b>	<b>7</b>
7.0.1 Introduction	7
7.0.2 Scope and Maturity	7
7.0.3 Applicable Regulations, Codes and Standards	7
7.0.4 Claims, Arguments and Evidence Route Map	8
<b>7.1 Overall Control &amp; Instrumentation</b>	<b>9</b>
7.1.1 Overall Architecture, Functions & Functional Allocation	9
7.1.2 Design Bases	9
7.1.3 Classification	21
7.1.4 C&I Building Layout	22
7.1.5 Prioritisation	23
7.1.6 ALARP, BAT, Secure by Design and Safeguards by Design	24
<b>7.2 Reactor Plant Control System</b>	<b>27</b>
7.2.1 System and Equipment Functions	27
7.2.2 Design Bases	27
7.2.3 Description	28
7.2.4 Materials	29
7.2.5 Interfaces	29
7.2.6 System and Equipment Operation	29
7.2.7 Instrumentation and control	29
7.2.8 Monitoring, Inspection, Testing and Maintenance	30
7.2.9 Radiological Aspects	30
7.2.10 Performance and Safety Evaluation	30
<b>7.3 Reactor Protection System</b>	<b>31</b>
7.3.1 System and Equipment Functions	31
7.3.2 Design Bases	31
7.3.3 Description	33
7.3.4 Materials	34
7.3.5 Interfaces	34
7.3.6 System and Equipment Operation	34
7.3.7 Instrumentation and control	34
7.3.8 Monitoring, Inspection, Testing and Maintenance	34
7.3.9 Radiological Aspects	35
7.3.10 Performance and Safety Evaluation	35
<b>7.4 Diverse Protection System</b>	<b>36</b>
7.4.1 System and Equipment Functions	36
7.4.2 Design Bases	36
7.4.3 Description	37
7.4.4 Materials	38
7.4.5 Interfaces	38
7.4.6 System and Equipment Operation	38
7.4.7 Instrumentation and control	39
7.4.8 Monitoring, Inspection, Testing and Maintenance	39
7.4.9 Radiological Aspects	39
7.4.10 Performance and Safety Evaluation	39



<b>7.5 Accident Management System</b>	<b>40</b>
7.5.1 System and Equipment Functions	40
7.5.2 Design Bases	40
7.5.3 Description	41
7.5.4 Materials	41
7.5.5 Interfaces	41
7.5.6 System and Equipment Operation	42
7.5.7 Instrumentation and control	42
7.5.8 Monitoring, Inspection, Testing and Maintenance	42
7.5.9 Radiological Aspects	42
7.5.10 Performance and Safety Evaluation	42
<b>7.6 Reactor Plant Monitoring System</b>	<b>43</b>
7.6.1 System and Equipment Functions	43
7.6.2 Design Bases	43
7.6.3 Description	43
7.6.4 Materials	44
7.6.5 Interfaces	44
7.6.6 System and Equipment Operation	44
7.6.7 Instrumentation and control	45
7.6.8 Monitoring, Inspection, Testing and Maintenance	45
7.6.9 Radiological Aspect	45
7.6.10 Performance and Safety Evaluation	45
<b>7.7 Other C&amp;I Systems</b>	<b>46</b>
7.7.1 Data Processing and Control System	46
7.7.2 Process Monitoring System	48
7.7.3 Feedwater, Steam and Condensate Control and Protection System	49
7.7.4 Turbine Island Control and Protection System	50
7.7.5 Cooling Water Island Control and Protection System	50
7.7.6 Water Supply Control and Protection System	51
7.7.7 Demineralisation Treatment Control and Protection System	51
7.7.8 Auxiliary Steam Generating System Control and Protection System	51
7.7.9 Security Management Systems	51
7.7.10 Building System Control	52
7.7.11 Communication and Information Systems	52
7.7.12 Instrumentation	52
<b>7.8 C&amp;I Essential Support Systems</b>	<b>54</b>
<b>7.9 Human Machine Interface</b>	<b>55</b>
7.9.1 Main Control Room	55
7.9.2 Supplementary Control Room	56
7.9.3 Emergency Response Centre	56
7.9.4 Technical Support Centre	56
7.9.5 Off-Site Emergency Response Centre	56
7.9.6 Local HMI Systems	57
<b>7.10 Conclusions</b>	<b>58</b>
7.10.1 ALARP, BAT, Secure by Design, Safeguards by Design	58
7.10.2 Assumptions & Commitments on Future Dutyholder/ Licensee / Permit Holder	58
7.10.3 Conclusions and Forward Look	58
<b>7.11 References</b>	<b>60</b>



<b>7.12 Appendix A: Claims, Arguments, Evidence</b>	<b>62</b>
<b>7.13 Glossary of Terms and Abbreviations</b>	<b>64</b>

**Tables**

Table 7.1-1: Allocation of C&I Systems to DiD Levels	10
Table 7.1-2: Qualification of C&I Systems	13
Table 7.1-3: C&I System Redundancies	14
Table 7.1-4: Independence within and between Systems	15
Table 7.1-5: Diversity within and between C&I Systems	18
Table 7.1-6: System Safety Integrity Objectives	19
Table 7.1-7: Spurious Failures per Annum (fpa) Objectives for Safety Systems	19
Table 7.1-8: C&I System Classifications	22
Table 7.2-1: RPCS [JSA] Safety Categorised Functional Requirements at DiD Level 2	27
Table 7.3-1: RPS [JRA] Safety Categorised Functional Requirements	31
Table 7.4-1: DPS [JQA] Safety Categorised Functional Requirements	36
Table 7.5-1: Allocation of Safety Class to PAMS [JRQ10] Variables	40
Table 7.12-1: Mapping of Claims to Chapter Sections	62

**Figures**

Figure 7.1-1: System Breakdown Structure for Reactor Island C&I [JY]	11
Figure 7.1-2: Reactor Island C&I Building Layout	23

## 7.0 Introduction to Chapter

---

### 7.0.1 Introduction

Chapter 7 of the Rolls-Royce Small Modular Reactor (RR SMR) generic Environment, Safety, Security and Safeguards (E3S) Case presents the overarching summary and entry point to the design information for the Control and Instrumentation (C&I) systems of the RR SMR. It is noted the terminology of ‘Control & Instrumentation’ is used interchangeably with the term ‘Instrumentation & Control’ used in International Atomic Energy Agency (IAEA) documentation.

### 7.0.2 Scope and Maturity

The scope of chapter 7 covers all C&I systems. This revision, at Version 2 of the generic E3S Case, focuses on the Reactor Island Control and Protection System [JY], with a brief summary of the other C&I systems. This revision also covers aspects of the RR SMR Human Machine Interfaces (HMIs).

The Reactor Island Control and Protection System [JY] includes the Reactor Protection System (RPS) [JRA], the Diverse Protection System (DPS) [JQA], the Accident Management System (AMS) [JRQ], and the Reactor Plant Control and Monitoring System (RPCMS) [JS], consisting of the Reactor Plant Control System (RPCS) [JSA] and the Reactor Plant Monitoring System (RPMS) [JSS].

The chapter covers the overall architecture for the Reactor Island Control and Protection Systems [JY], including the allocation of functional and non-functional safety requirements to specific systems. It also includes a description of specific C&I systems being designed to achieve their requirements, and how the design is being developed to reduce risks to as low as reasonably practicable (ALARP), apply best available techniques and in line with secure by design and safeguards by design.

Version 2 of the generic E3S Case is based on reference design 7 (RD7), corresponding to design reference point 1 (DRP1) for the generic design assessment (GDA). At RD7/DRP1, the safety functions to be delivered by each structure, system and component (SSC) are presented, with the assignment of safety categorised functional requirements to achieve them. No functional requirements for environment, security and safeguards are identified for SSCs in the scope of chapter 7 at DRP1/RD7, noting SSCs are designed in accordance with E3S and engineering processes that include development against principles for environment, security, and safeguards. The design definition presented is based on the design maturity of each respective SSC at RD7/DRP1. Verification and validation activities for SSCs within this chapter are still to be established in future revisions of the generic E3S case.

### 7.0.3 Applicable Regulations, Codes and Standards

The RR SMR C&I Codes and Standards Selection Report [1] lists the codes, standards and legislation which is being used to develop the RR SMR C&I systems design. It also details the process for selecting the standards and the applicability of the standards to the systems of different safety classes.



## 7.0.4 Claims, Arguments and Evidence Route Map

The overall approach to claims, arguments, evidence (CAE) and the set of fundamental E3S claims to achieve the E3S fundamental objective are described in E3S Case Version 2, Tier 1, Chapter 1: Introduction [2]. The top-level claim for E3S Case Version 2, Tier 1, Chapter 7: Instrumentation and Control is:

***Claim 7: Instrumentation and Control systems are conservatively designed and verified to deliver E3S functions through-life, in accordance with the E3S design principles, to reduce risks to ALARP, apply BAT and in line with Secure-by-Design and Safeguards-by-Design.***

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

A proportionate summary of the arguments and evidence from lower tier information, available at the current design stage, RD7/DRP1, is presented within this chapter. A mapping of the claims to the corresponding sections that summarise the arguments and/or evidence is provided in Appendix A (section 7.12).

## 7.1 Overall Control & Instrumentation

### 7.1.1 Overall Architecture, Functions & Functional Allocation

The deterministic safety analysis presented in E3S Case Version 2, Tier 1, Chapter 15: Safety Analysis [4], provides a systematic evaluation of the credible postulated initiating events (PIEs). High level safety functions (HLSFs) are identified in the Fault Schedule [5] and assigned to each PIE to deliver the four fundamental safety functions (FSFs): control of reactivity (CoR), control of fuel temperature (CoFT), confinement of radioactive material (CoRM) and control of radiation exposure (CoRE).

Safety measures are specified across each level of defence-in-depth (DiD) to prevent, protect, or mitigate against each PIE and deliver the HLSF. A safety measure represents the totality of SSCs needed to deliver the HLSF, which includes the C&I systems that deliver the C&I functions.

As such, the Reactor Island C&I architecture aligns with the DiD levels in the Fault Schedule, allowing for the allocation of C&I safety functions to different C&I systems based on Fault Schedule allocation to preventative, protective 1 and protective 2, and mitigation safety measures. The C&I systems for each level of DiD are described in section 7.1.2.

The C&I architecture describes the interconnection of all the systems and the interfaces between them. It reflects the way the overall C&I system is thought about in terms of its structure, functions, and relationships. C&I functions are assigned to the individual C&I systems in the architecture, so that appropriate non-functional system requirements (classification, redundancy, reliability, etc.) can be allocated to the individual C&I systems.

A detailed description of the Reactor Island Control and Protection System [JY] is presented in the System Design Description – Reactor Island Control and Protection Systems [6], and summarised in this chapter.

### 7.1.2 Design Bases

#### 7.1.2.1 Functional requirements

The C&I safety functional requirements are listed in the Reactor Island Control and Protection System [JY] modules of the RR SMR requirements management database. The C&I Engineering Schedule [7] supports the allocation of the safety functional requirements by arranging C&I safety functions into appropriate DiD groups.

#### 7.1.2.2 Non-functional requirements

The design rules to be used in development of the C&I systems are summarised below. These design rules are defined as non-functional system requirements and applied to individual C&I systems through their requirements module in the RR SMR requirements management database.

##### 7.1.2.2.1 Defence-in-Depth

The five levels of DiD for the RR SMR are described in E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules [8] with DiD level 1 and 2 measures providing normal duty operation and response to anticipated operational occurrences, level 3 protective measures providing

protection in response to faults, level 4 providing mitigative measures following escalation of a fault, and level 5 providing emergency response measures. Independent and diverse C&I systems are required to provide DiD. For RR SMR, this comprises:

- The DPS [JQA], is a hardwired (i.e., non-programmable electronics) system providing the primary means of reactor protection. The DPS is the primary means of implementing DiD level 3 category A functions.
- The RPS [JRA], a nuclear-qualified ‘complex’ technology (i.e., programmed electronics) enabling the benefits of complex functions to be used in the calculation of protection trip functions and actuation of Engineered Safety Features (see E3S Case Version 2, Tier 1, Chapter 6: Engineered Safety Features [9]). The RPS is the secondary means of implementing DiD level 3 category A functions.
- The AMS [JRQ], consisting of Post Accident Management System (PAMS) and Severe Accident Management System (SAMS), that support all nuclear accident management systems. In the event of a serious incident, an Emergency Response Centre is also available to enable management of an emergency response, including coordination of on-site and off-site emergency response teams. The AMS [JRQ] is responsible for delivering both the DiD level 3 and DiD level 4 functions via the PAMS [JRQ10], and the SAMS[JRQ20], respectively.
- The RPCS [JSA], a second programmable electronics system that is diverse from the RPS [JRA] and provides reactor control functions. The RPCS [JSA] is part of the overall Reactor Plant Control and Monitoring System (RPCMS) [JS]. The Reactor Plant Control System [JSA] is responsible for delivering both the DiD level 1 and DiD level 2 functions via the Reactor Control System [JSA10], and the Reactor Limitation & Preventive Protection System [JSA20] respectively. The Control Rod Control System (CRCS) [JSA30] is likely to deliver DiD level 1 and DiD level 2 functions (the CRCS controller will perform prioritisation of rod control between DiD level 1 and DiD level 2 programmable logic controllers (PLCs) inputs).
- The RPMS [JSS], monitoring the non-safety critical parameters of the reactor to provide condition monitoring. The RPMS [JSS] together RPCS [JSA] form the overall Reactor Plant Control & Monitoring System (RPCMS) [JS]. The RPMS [JSS] is responsible for delivering DiD level 1 functions.

The DiD levels of the C&I systems are summarised in Table 7.1-1.

**Table 7.1-1: Allocation of C&I Systems to DiD Levels**

DiD Level	C&I System
1	Reactor Control System [JSA10]
1 and 2	Control Rod Control System [JSA30]
1	Nuclear HVAC Supervisory Control System [JSA40]
1	Reactor Plant Monitoring System [JSS]
2	Reactor Limitation & Preventive Protection System [JSA20]
3	Reactor Protection System [JRA]
3	Diverse Protection System [JQA]

<b>DiD Level</b>	<b>C&amp;I System</b>
3	Post-Accident Management System [JRQ10]
4	Severe Accident Management System [JRQ20]
5	Emergency Response Centre HMI

The individual C&I systems, or sub-systems, comprising the Reactor Island Control and Protection System [JY] are presented in Figure 7.1-1.



**Figure 7.1-1: System Breakdown Structure for Reactor Island C&I [JY]**

### 7.1.2.2 Qualification

Qualification procedures are applied to confirm that structures, systems, and components will perform their allocated safety function(s) in all normal operational, fault and accident conditions identified in the safety case and for the duration of their operational lives.



Qualification for the C&I equipment generally follows the requirements of standard BS EN IEC 60780-323:2017 – Nuclear facilities – Electrical equipment important to safety – Qualification, the standard is applicable to electrical equipment important to safety and its interfaces that are necessary to perform a safety function, or whose failure could adversely affect the safety functions of other equipment.

Qualification is based on a selection of methods, with the specific combination of methods being selected appropriate to the particular system or component:

- Use of engineering and manufacturing processes in compliance with recognized standards
- Reliability demonstration
- Past experience in similar applications
- Type tests
- Testing of supplied equipment
- Analysis for extrapolating test results or operating experience under relevant conditions
- Evaluation of manufacturer production processes
- Inspection of components during manufacture.

For safety systems, evidence of qualification on the basis of operating experience is insufficient and is, therefore, combined with type testing and testing of supplied equipment, as well as with evaluation of the design and development processes of manufacturers or inspection of components during manufacture. This follows a two-legged approach involving production excellence (PE) assessment, which will incorporate the independent assessment and compensating activities and independent confidence building measures (ICBMs) which will focus exclusively on the demonstration of fitness for purpose.

The qualification programme addresses all topics affecting the suitability of each system or component for its intended functions. Qualification of each system is expected to include but is not limited to the following:

- Environmental qualification
- Qualification for the effects of internal and external hazards
- Electromagnetic qualification
- Suitability and correctness of functions and performance
- Assessment of performance over expected lifetime

The qualification of C&I Systems is presented in Table 7.1-2.

**Table 7.1-2: Qualification of C&I Systems**

C&I System	RPCS	RPS	DPS	AMS
Equipment Qualification	Y	Y	Y	Y
Seismic	-	Y	Y	Y
EMC	Y	Y	Y	Y
Lifecycle (application)	Y	Y	Y	Y
Lifecycle (platform)	Y	Y	Y	Y
Lifecycle (smart devices)	Y	TBD	N/A	TBD

Qualification is performed against the requirements of the standards identified according to the system classifications.

The requirements and rigour required to qualify systems and equipment is graded according to the classification of the individual C&I systems and equipment.

### 7.1.2.2.3 Failure Behaviour

The concept of fail-safe design is incorporated, as appropriate, into the design of systems and components important to safety. Consequently, a loss of power to any C&I component is designed to place the affected system into a predefined condition that is demonstrated to be acceptable for safety (i.e. taking redundancy, and both failure on demand and spurious actuation of the safety function into account, with an appropriate balance between the two adapted to the particular safety functions and systems, and recognising that some actuators do not have a 'safe state' that is applicable to all conditions - e.g. containment isolation valves).

Systems are designed to fail to a safe condition for their most probable known failure modes, or when de-energised, and to use 'watchdog timers' to detect that equipment is no longer performing its design function and to place the system in a safe condition.

Safety Systems that perform reactor trip functions de-energise on failure and the safe state is actuated (i.e. tripped). Safety Systems that initiate protective measures de-energise on failure and the safe state is not actuated (i.e., to reduce the probability of inadvertent actuation).

C&I systems are designed with self-diagnostics to ensure that detectable faults are revealed as soon as possible, and those that may not be revealed by self-diagnostics or alarms are detectable by periodic testing, or by routine surveillance of anomalous indications. Self-test facilities are designed in accordance with the self-supervision requirements of the codes & standards relevant to their classification.

### 7.1.2.2.4 Redundancy

All Reactor Island [R01] safety class 1 and class 2 safety systems have redundant divisions.

Class 1 systems are designed for compliance with the single failure criterion (SFC) with the provision of four independent redundancies. This arrangement assures that the safety function can be delivered in the presence of a single failure and un-availability of a whole redundancy for



maintenance. Loss of a redundancy of a class 1 C&I System due to an initiating event is not assumed at this stage in the design – this is to be confirmed through future detailed hazards analysis.

Deterministically, class 2 systems are not expected to comply with the single failure criterion, and therefore a minimum of two redundancies are required. However, the RPS [JRA] is designed with three redundancies to further reduce risks associated with probability of failure on demand and spurious actuation and because in several cases the underlying fluid/mechanical system, which is controlled, consists of 3 redundancies.

Class 3 and non-classified systems do not need to have redundant elements for reasons of safety, but the Reactor Island duty systems are redundant where failure/disturbance could lead to loss of generation and/or place frequent demands on safety systems.

The C&I System redundancies at RD7/DRP1 are provided in Table 7.1-3.

**Table 7.1-3: C&I System Redundancies**

C&I System	Redundancy
DPS	4 (SFC compliant)
RPS	3
SAMS	2
PAMS (Type B and C variables)	3
PAMS (Type D and E variables)	TBD
RPCS	N+1 (Duty and Standby)
RPMS	N

#### **7.1.2.2.5 Independence**

The C&I systems design will provide independence in the following cases:

- Independence between systems of different safety classes, specifically to prevent failure propagation from lower to higher classified systems
- Independence between systems of different DiD layers
- Independence between the first protective safety measure and the second protective safety measure
- Independence between redundancies of a particular system, to prevent propagation of a failure, an internal hazard, or an external hazard between redundancies. This independence is also maintained between the redundancies of the essential support services of the class 1 and class 2 systems
- Independence between the HMI in the Main Control Room from the HMI in the Supplementary Control Room (SCR), to prevent failures in one of the rooms from defeating the HMI in the other



- Sensor sharing is only allowed in cases where it does not defeat independence. Signal sharing policy is applied to the design in order to maintain the necessary independence of redundant systems and between different systems.

When independence is required, it should be achieved by using:

- Physical separation, which can be achieved by distance, barriers, or a combination of the two.
- Electrical isolation, which can be achieved by fibre optics, optical isolators, cable shields, or other isolation equipment
- Independence of communication for computer based systems, which can be achieved by selecting appropriate data communication architectures, protocols, and gateways between networks.

Independence of power supplies for C&I systems at different DiD levels is also implemented. E3S Case Version 2, Tier 1, Chapter 8: Electrical Power [10] details how this is achieved.

The outcome of this is summarised in Table 7.1-4.

**Table 7.1-4: Independence within and between Systems**

System A	System B	Physical separation	Electrical independence	Communication independence
Division X	Division Y	Room for class 1 and class 2 systems	Electrical isolation	Inter-redundancy independence (1-way & voted)
RPS	DPS	Room	Electrical isolation	No communication except priority logic
RPS	DPCS	Room	Electrical isolation	1-way (A to B) at physical level
RPS	SAMS	Room	Electrical isolation	No communication
RPS	PAMS	None required	None required	None required
DPS	DPCS	Room	Electrical isolation	1-way (A to B) at physical level
DPS	SAMS	Cabinet	Electrical isolation	1-way (A to B) at physical level
DPS	PAMS	Room	Electrical isolation	1-way (A to B) at physical level
SAMS	RPCMS	Room	Electrical isolation	1-way (A to B) at physical level
PAMS	RPCMS	Room	Electrical isolation	1-way (A to B) at physical level

In Table 7.1-4, PAMS refers to the equipment for monitoring types B and C Variables.



Physical separation is required to protect against hazards and is strongly linked to the layout safety justification. The assumption at RD7/DRP1 is that the systems will be separated so that the duty and safety systems are physically separated, and so that the redundant safety system divisions are physically separated (i.e., so that an internal or external hazard can affect at most one redundancy). The conclusions from the high-level probabilistic safety assessment (PSA) were that if essential equipment cannot be completely segregated, it is more important to ensure that each train of an essential system is segregated than to ensure that each essential system is segregated from other essential systems. However, the conclusions also noted that it was possible to achieve almost two orders of magnitude benefit by complete segregation of essential equipment, and hence segregation of RPS and DPS equipment (at minimum with a significant fire barrier – e.g., sub-divided rooms with 8- or 12-hour fire barrier; and noting that independent Heating, Ventilation and Air Conditioning (HVAC) may also need to be provided) is judged desirable at this stage of the design.

### 7.1.2.2.6 Common Cause Failure and Diversity

Independence, redundancy and diversity are applied across the overall C&I architecture to address the requirement on CCF mitigation.

The C&I architecture is designed around three platforms using three different technologies and procured from three different manufacturers:

- The first platform is based on a non-programmable technology and forms the DPS [JQA]. It is the primary means of implementing all DiD level 3 category A C&I functions and is thus class 1. This hardwired platform is also used to implement the SAMS, which performs the DiD level 4 mitigating functions. Even though the DPS and the SAMS use the same technology, the systems will be independent from each other and will employ function and signal diversity.
- The second platform consists of complex programmable technology. This platform takes advantage of modern technology to implement more complex algorithms, provide greater equipment density and utilise digital networks to simplify cabling. This platform forms the RPS [JRA]. It is the secondary means of implementing the DiD level 3 category A C&I functions and the primary means of implementing all the category B C&I functions. This is a class 2 system. For the category A functions, diverse initiating parameters are used between the RPS and the DPS as far as is reasonably practicable. This platform can also be used to implement PAMS functions.
- The third platform also utilises complex programmable technology but utilises a diverse technology from the second (RPS) platform. This platform is used to implement the Preventive Safety Measures, which are provided in DiD level 2. This platform also forms the basis for all the duty (DiD level 1) C&I like the RPCMS, Radwaste C&I and Fuel Route C&I. This platform implements category C or non-classified functions and is class 3. Platform standardisation will be applied as much as possible, but there may be instances for specialised systems where an alternative platform will be used. Any alternative platforms will meet the same requirements as the ‘standardised’ class 3 platform.

Several different types of diversity are provided within the design:

- Design diversity: Use of different technologies and different design approaches to solve the same problem



- Equipment manufacturer diversity: Use of different sources of the hardware components or aggregate system
- Logic processing equipment diversity: Use of different types of logic processing equipment employed
- Functional diversity: Systems perform different functions to achieve the same safety outcome
- Life-cycle diversity: Focus on human resources during the life-cycle
- Logic diversity: Use of different logic description languages, different algorithms, different timings, different sequencing of logical functions
- Signal diversity: Safety action is initiated based upon different plant parameters.

The diversity between C&I Systems are indicated in Table 7.1-5. In the table PAMS refers to the equipment for monitoring types B and C variables (in accordance with BS EN 63147). Allocation of safety category and safety class to PAMS variables is summarised in the System Design Description [6]. At RD7/DRP1, it is not yet defined if independent or diverse sensors are necessary or are available, where indicated with an asterisk symbol (\*) in Table 7.1-5. However, as a minimum, any sensors used for protection against postulated initiating events will not also be used for control purposes that could cause those same events. Similarly, as far as is practicable, diverse means of detection will be used between the protection systems to detect each postulated initiating events. Where diverse signals use is not practicable, each protection system shall utilise its own sensors to sense the parameter.

**Table 7.1-5: Diversity within and between C&I Systems**

System A	System B	Design diversity	Manufacturer diversity	Logic diversity	Functional diversity	Life cycle diversity	Logic diversity	Signal diversity
DPS	RPS	Y	Y	Y	Y	Y	Y	Y
DPS	RPCMS	Y	Y	Y	Y	Y	Y	Y*
DPS	SAMS	Not required						
DPS	PAMS	Not required						
RPS	RPCMS	Y	Y*	Y	Y	Y	Y	Y*
RPS	SAMS	N	Y	N	N	N	N	Y
RPS	PAMS	Not required						
RPCMS	SAMS	N	Y	N	N	N	N	Y
RPCMS	PAMS	Y	Y	TBD	Y	Y	Y	Y
SAMS	PAMS	Y	Y	Y	TBD	Y	Y	Y
Priority Logic A	Priority Logic B	N	Y	N	N	Y	N	N



### 7.1.2.2.7 Reliability

The reliability requirements placed on the C&I systems are commensurate with the safety significance of the individual systems, presented in Table 7.1-6.

**Table 7.1-6: System Safety Integrity Objectives**

C&I System	RPCS	RPS	DPS	SAMS	PAMS
Safety function	1E-1 failures per annum (fpa)/ probability of failure per demand (pfд) (including RLPPS)	1E-3 pfд	1E-4 pfд	1E-1 fpa/pfд	1E-3 fpa for the class 2 equipment

Table 7.1-6 presents an initial safety limit for SAMS. In practice, it is expected to have higher reliability.

Design techniques such as testability, including a self-checking capability where necessary, fail-safe characteristics, functional diversity and diversity in component design are used to the extent practicable in the design to prevent the loss of a safety function.

The C&I systems are also designed for high functional reliability and periodic testability commensurate with the safety functions they perform.

### 7.1.2.2.8 Spurious Failure

The RPS is assumed to have a target frequency of spurious actuation causing a significant transient of  $\leq 1E-3/\text{year}$ . The DPS is assumed to have a target frequency of spurious actuation causing a significant transient of  $\leq 1E-5/\text{year}$ . The plant design impacts on this criterion where there may be mechanical/process interlocks provided that prevent the transient.

For plant availability reasons RPS and DPS are assumed to each have a target frequency of spurious actuation that does not cause a significant transient of  $\leq 1E-2/\text{year}$ .

The C&I systems are designed to satisfy the criteria as listed in Table 7.1-7.

**Table 7.1-7: Spurious Failures per Annum (fpa) Objectives for Safety Systems**

C&I System	RPCS	RPS	DPS	SAMS
Spurious failures per annum	1E-1 fpa	1E-3 fpa for a failure leading to a significant transient	1E-3 to 1E-5 fpa for a failure leading to a significant transient	1E-1 fpa



### 7.1.2.2.9 Examination, maintenance, inspection & testing

Maintenance of the C&I Systems ensures they remain safe to operate and meet their operating targets through life.

The examination, maintenance, inspection & testing (EMIT) strategy informs the design for EMIT maintenance activities on the C&I systems, including the DPS and RPS. Redundancy is incorporated into the design to facilitate EMIT, at a frequency informed by PSA. The C&I systems incorporate built-in test features, to enable automated, online testing to be carried out during operation. This is supplemented by manual testing and maintenance, as appropriate.

The C&I Design for EMIT strategy report [11] identifies non-functional requirements for EMIT from standards, SMR internal requirements and RGP to inform the design for EMIT maintenance activities on C&I control systems.

### 7.1.2.2.10 Human Machine Interface

The RR SMR control room design uses established C&I architecture and technology based on review of operational experience (OPEX), relevant good practice (RGP) and new reactor designs across the nuclear industry. The architecture includes provision for the HMI design to meet Human Factors requirements for an information rich interface to facilitate delivery of the role of the operating personnel. The control room HMIs will primarily be computerised, but a small set of important safety displays and controls will provide a simple and robust hardwired backup.

### 7.1.2.2.11 Security

The overall C&I architecture ensures that the Reactor Island Control and Protection Systems are independent and segregated from each other to the extent defined in section 7.1.2.2.4 and 7.1.2.2.5. In particular the DPS is independent from the other systems that are of lesser importance to safety. The design provisions that address this are generally also helpful in meeting the security requirements.

The design provisions for diversity, not least the provision in the design of a simple hard-wired protection system, will enable development of the means of restricting data access to authorised individuals, establish security measures to keep information safe and are also helpful in addressing cyber security concerns.

To the extent possible, the design ensures that access, security, cyber-security and safety requirements are addressed so that they do not compromise one another. Careful design should ensure that neither operation nor failure of any computer security function will adversely affect the ability of a system to perform its safety function. Similarly, complexity introduced by security controls does not degrade the C&I system response time. The C&I Safety and Cyber Security Integration Strategy [12] provides more detail on the integration of security, safety and design.

The highest security degree is allocated to the hardwired class 1 DPS, backed up by a programmable RPS, both with enforced one-way communications through a gateway to the plant network. A simple hard-wired DPS provides added protection to satisfy cyber security concerns.

One-way communications are also enforced from the RPS systems (performing category A functions, and so also at security degree 1, but in a different zone to the DPS) to other RPS systems (performing category B functions and defined as security degree 2).

All systems and data connections for systems and components are inside cabinets. Physical access is controlled to both the rooms in which the cabinets are located, and to the inside of the enclosures by locked doors. Indication of access to protection system cabinets and of any operational bypasses is provided in the control room. All unused data connections are disabled. Provisions are provided to control test, maintenance or calibration equipment that may be connected.

### 7.1.3 Classification

The E3S Categorisation & Classification methodology is described in E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules [8], with its application to mechanical SSCs presented in various engineering chapters across the E3S case. The approach adopted is consistent with BS IEC 61226 [13]. The Reactor Island Control and Protection Systems are classified correspondingly to the functions they perform:

- RPCMS is a class 3 system and performs the duty control and monitoring functions for the reactor island systems (neutronic power, primary pressure, Reactor Coolant Pumps (RCP), Steam Generators (SG) levels etc.) and the category C preventative functions, provides the rod control functions, Nuclear HVAC Supervisory Control System and non-safety monitoring functions.
- RPS is a class 2 system because it is the primary means to implement category B safety functions and is the secondary means to implement category A functions.
- DPS actuates the primary category A safety functions and is class 1.
- PAMS provides support to operators during design basis accidents. The functions and the associated safety class of the PAMS is derived from standards, rather than from allocated safety functions. Notably, BS IEC 63147:2017 [14] and the Guidance for the application of IEC 63147:2017 [15] are used to establish safety classes for the different types of variables to be monitored by the PAMS, as described in section 7.5.2.3.1.
- SAMS provides C&I functionality dedicated to the management of Severe Accidents in DiD level 4. C&I functions which mitigate Design Extension Conditions (DEC) or Severe Accidents are assigned to the SAMS. In accordance with E3S Categorisation and Classification methodology [16] the SAMS is assigned to class 3.
- The Radwaste C&I and the Fuel Route C&I are expected to perform duty category C functions and is assigned to class 3.

The classification of the C&I systems is summarised in Table 7.1-8. Ongoing work beyond RD7/DRP1 may result in a redistribution of some of the PAMS functionality to other systems.

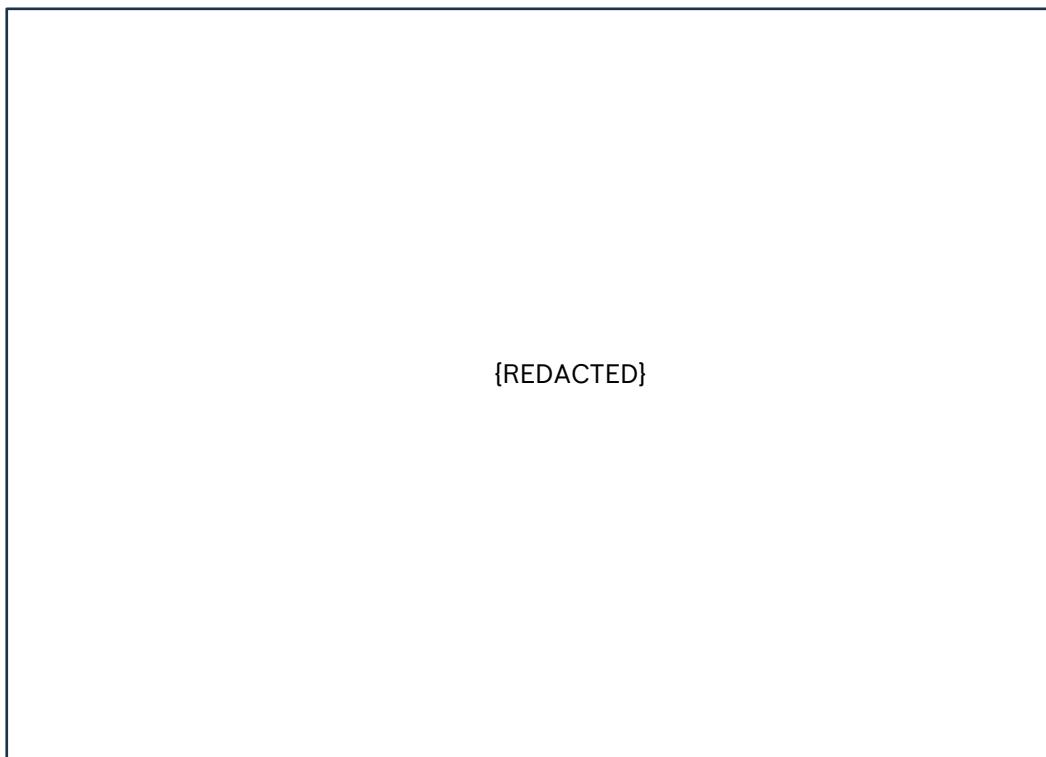
**Table 7.1-8: C&I System Classifications**

C&I System	Safety Class
RPCMS [JS]	3
RPS [JRA]	2
DPS [JRQ]	1
PAMS [JRQ10]	2
SAMS [JRQ20]	3

## 7.1.4 C&I Building Layout

The locations of the equipment of the Reactor Island C&I are shown in Figure 7.1-2. The DPS [JQA], RPS [JRA], and AMS [JQR] are all located on an aseismic bearing under the Hazard Shield. The Main Control Room (MCR) is also located in the building housed under the Hazard Shield. The C&I Systems are:

- DPS [JQA] – four divisions in four EC&I clusters (referred to as EC&I ‘trains’ in Figure 7.1-2) segregated by civil structures in the Hazard Shield
- RPS [JRA] – three divisions in three of the EC&I clusters segregated by civil structures in the Hazard Shield
- PAMS [JRQ10] – three divisions in three EC&I clusters segregated by civil structures, closely integrated with RPS in the Hazard Shield
- SAMS [JRQ20] – two divisions in two of the EC&I clusters segregated by civil structures in the Hazard Shield
- Control Rod Control System [JSA30] – in one of the EC&I clusters inside the Hazard Shield
- Reactor Plant Control Systems [JSA10], [JSA20], [JSA40] – co-located with [JSA30] at RD7/DRP1 but post-RD7/DRP1 optimisation might place them in the Access Block part of the Support Building, outside the Hazard Shield and off the Seismic Isolation System
- Reactor Plant Monitoring System [JSS] - in the Access Block part of the Support Building, outside the Hazard Shield and off the Seismic Isolation System.



**Figure 7.1-2: Reactor Island C&I Building Layout**

Physical separation, Modular Kit of Parts (MKoP) barriers and civil structures are used for segregation between safety systems or between redundant elements of a system.

## 7.1.5 Prioritisation

A prioritisation ranking is needed to arbitrate conflicting demands on shared actuators from C&I systems at different levels of DiD.

The priority order identified at RD7/DRP1 is as follows:

1. Essential Component Protection - implemented within the switchgear
2. Local Manual Control – implemented within the switchgear or at the actuator directly
3. Diesel Generator management (Load shedding) – implemented in C&I Systems
4. Actions requested for safety functions:
  - a. Priority of the safety actuation should be determined first by the Safety function category, with the highest category, category A, have the highest priority.
  - b. Where the same function category is enacted by two systems, the higher classification system shall take priority.
  - c. Within a, and b, there are sub-categories for detailed prioritisation:



- i. Where functions have the same category and classification, demands in the safe direction of the actuator shall take priority over an equivalent priority signal in the other direction.
  - ii. Automatic commands should be prioritised over manual commands of unclear priority.
5. Non-essential component protection – implemented in C&I systems
  6. Duty Control

At RD7/DRP1 it is assumed that the long-term commands to reset the safety systems will be given by operators from the manual control switches in the main control room (MCR) or the supplementary control room (SCR).

The functional concept has the following features:

- Priority Logic System (PLS) activities are incorporated into separate Priority Logic Units (PLU), located anywhere on the plant that meets environment, hazard and separation/independence requirements.
- Local Manual Control is routed directly to the switchgear, bypassing the PLS.
- Translating functions to actuator demands (Fan out), occurs at convenient location for layout and C&I, before any signals are sent to the PLUs.
- Duty and preventative functions are prioritised within the class 3 C&I system before fan out. RPS category A Functions are sent to the DPS PLS to translate into actuator instructions because they are duplicate functions doing the same actuation.
- Actuator status is produced by switchgear or motorised actuator feedback systems and are assumed to be processed within C&I systems. The exact flow of status signals within the C&I systems has not yet been determined.
- Motorised actuator feedback loop is considered detachable and can be located at switchgear/actuator/PLU. It is assumed to be located at the switchgear.
- Safety functions are latched within each C&I System or control room at the point they are demanded/tripped before fan out with reset signals assumed to come from operators in the control rooms.
- Control room demands go directly to the PLU units except in the case of Duty functions.

## 7.1.6 ALARP, BAT, Secure by Design and Safeguards by Design

The overall design of the Reactor Island C&I Systems [JY] has been developed in accordance with the systems engineering design process, which includes alignment to RGP and OPEX, including design rules outlined in section 7.1.2.2, design to codes and standards according to the safety classification, and a systematic optioneering process with down-selection of design options based on assessment against relevant E3S criteria (as described in E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules [8]).



The key design decisions with respect to ensuring overall risks are reduced to ALARP are summarised below. Further ALARP aspects specific to individual C&I systems are also described in subsequent sections of this chapter.

### 7.1.6.1 Overall C&I Design

The general nuclear C&I design is being developed as separate sub-systems for Reactor Island C&I, Fuel Route C&I and Waste Management C&I, on the basis that there is only minimal interaction between them. This approach aligns to RGP seen in other reactor designs.

### 7.1.6.2 Reactor Island C&I Defence-in-Depth

The Reactor Island C&I architecture has been developed to align with the DiD levels in the Fault Schedule [5], allowing for the allocation of safety functions to different systems based on Fault Schedule allocation to duty, preventative, protective 1 and protective 2, and mitigative safety measures.

This architecture minimises the need for priority logic by locating safety functions that drive common actuators in the same system, where possible. It also ensures that independence can be maintained between the safety functions identified against each PIE on the same line of the Fault Schedule but are at different levels of defence-in-depth.

The hardwired DPS [JQA] provides independence and a diverse platform to the RPS [JRA] to perform all category A functions. The implementation of two diverse systems at DiD level 3 meets United Kingdom (UK) RGP for frequent faults, which are expected to be detected and accommodated by two diverse protection systems. This architecture is also in line with UK expectations that class 1 protection systems will employ diversity in their detection of and response to fault conditions.

Optioneering of system architectures for performing preventive functions has been undertaken, including options for a combined system with the RPS [JRA], a standalone preventive system, or allocation of preventive functions across the other software-based systems. The provision of a separate system (Reactor Limitation and Preventive Protection System [JSA20]) has been selected as design baseline, as it offers independence to other systems across the levels of DiD to ensure functional diversity, minimising the potential of CCFs impacting both DiD levels 2 and 3.

### 7.1.6.3 Redundancy in Class 1 & 2 Systems

At RD7/DRP1, the DPS [JQA] (class 1) has four redundancies while the RPS [JRA] (class 2) has three redundancies. Class 1 systems are designed for compliance with the SFC with the provision of four independent redundancies. This arrangement assures that the safety function can be delivered in the presence of a single failure and un-availability of a whole redundancy for maintenance. Loss of a redundancy of a class 1 C&I system due to an initiating event is not assumed at this stage in the design – this is to be confirmed through future detailed hazards analysis. Class 1 C&I equipment shall be appropriately protected from the effects of a PIE and qualified to the expected environmental conditions. In cases where a fluid/mechanical system design has only two redundant actuators, the C&I equipment from the voting logic “downwards” cannot be tested during plant operations in compliance with the SFC (Priority logic, Electrical switchgear, valves). For these cases, a risk trade-off will be performed between testing (non-compliant to SFC) to find failures or no testing to remain SFC compliant. In cases where a fluid/mechanical system design has only one C&I controlled actuator; the C&I System cannot achieve the SFC by itself. In these cases, the SFC is achieved at the higher level, which usually includes other mechanical provisions like non-return valves.



Deterministically, class 2 systems are not expected to comply with the SFC, and therefore a minimum of two redundancies are required. However, the RPS [JRA] is designed with three redundancies to further reduce risks associated with pfd and spurious actuation.

#### 7.1.6.4 Priority Logic

For all actuators controllable by the DPS [JQA] or RPS [JRA], PLUs shall feature diversity between trains to mitigate CCF in the category A functions. The class 1 PLUs shall have at least one design that is based in hardwired technology. This decision was made to drive conservatism in the design, ensuring that independence and diversity built into the wider plant architecture is not defeated by the prioritisation approach, which is the 'final link in the chain' to the actuator. It is also consistent with RGP over options to use software-based prioritisation for the DPS [JQA] and RPS [JRA], which have the potential to introduce CCFs. Prioritisation between the Reactor Control System (RCS) [JSA10] and the Reactor Limitation and Preventive Protection System (RLPPS) [JSA20] will be done via software.

#### 7.1.6.5 Layout

Optimisation of the C&I systems located within the Hazard Shield has been undertaken to ensure appropriate protection against seismic and aircraft impact external hazards. The RD7/DRP1 design includes the DPS [JQA], RPS [JRA], and AMS [JRQ] positioned under Hazard Shield, as well as the associated battery back-up, switch room electrical equipment and HVAC. This ensures all class 1 and class 2 systems remain available and minimises the number of penetrations required in the Hazard Shield, with class 3 and non-classified systems located outside the Hazard Shield to minimise the overall footprint.



## 7.2 Reactor Plant Control System

### 7.2.1 System and Equipment Functions

The RPCS [JSA] is a sub-system of the RPCMS [JS].

The primary function of the Reactor Plant Control System [JSA] is to provide process control and monitoring of the primary reactor systems and associated heat exchangers.

During normal operating conditions the RPCS [JSA] delivers duty functions designed to maintain control of the process parameters of the primary reactor systems and associated heat exchangers within their normal operating conditions. During abnormal operating conditions, the Reactor Limitation and Preventive Protection System [JSA20], a sub-system of the Reactor Plant Control System [JSA], 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.

### 7.2.2 Design Bases

#### 7.2.2.1 Functional requirements

The RPCS [JSA] facilitates the delivery of nuclear heat removal during normal operation. Safety categorised functional requirements allocated to the RPCS [JSA] based on the HLSFs they deliver, including the applicable plant states, are presented Table 7.2-1. The functional requirements in Table 7.2-1 correspond to the allocated protective and preventative measures from the Engineering Schedule [7], delivered by the Reactor Limitation and Preventive Protection System [JSA20]. Functional requirements for DiD level 1 duty functions are still in development.

**Table 7.2-1: RPCS [JSA] Safety Categorised Functional Requirements at DiD Level 2**

Functional Requirement	Plant State(s)	Safety Category
When demanded, the [JSA] System shall Limit Rod Withdrawal Speed	DBC-2i	C
When demanded, the [JSA] System shall Initiate Condenser Decay Heat Removal (DHR)	DBC-2i	C
When demanded, the [JSA] System shall Control Auxiliary Steam Generator Feed	DBC-2i	C
When demanded, the [JSA] System shall Initiate Atmospheric Steam Dump (ASD) Cooldown	DBC-2i	C
When demanded, the [JSA] System shall initiate Reactor Power Runback	DBC-2i	C
When demanded, the [JSA] System shall Trip Pressuriser Heaters	DBC-2i	C
When demanded, the [JSA] System shall Trip Pressuriser Spray	DBC-2i	C



Functional Requirement	Plant State(s)	Safety Category
When demanded, the [JSA] System shall initiate Main Steam Isolation	DBC-2i	C
When demanded, the [JSA] System shall initiate transition to House-load supply	DBC-2i	C
When demanded, the [JSA] System shall Auto Stop Chemical and Volume Control System (CVCS)	DBC-2i	C
When demanded, the [JSA] System shall Trip Cold Shutdown Cooling System (CSCS) on overcooling	DBC-2i	C

The safety functional requirements are consolidated in the Reactor Island Control and Protection Systems [JY] module in the RR SMR requirements management database which are then allocated where appropriate to the Reactor Plant Control System [JSA] requirements module.

### 7.2.2.2 Non-functional requirements

The non-functional requirements are consolidated in the Reactor Island Control and Protection Systems [JY] module in the RR SMR requirements management database, based on the design rules listed in section 7.1.2.2, and are then allocated where appropriate to the Reactor Plant Control System [JSA] RR SMR requirements module. Some non-functional requirements are allocated unaltered, while others require further decomposition, potentially on analysis, such as cross C&I system diversity and independence requirements.

### 7.2.2.3 E3S classification

#### 7.2.2.3.1 Safety Classification

The highest safety category of functions delivered by the RPCS [JSA] at RD7/DRP1 is category C.

The RPCS [JSA] and all its defined subsystems have an overall preliminary safety classification of class 3, according to the E3S Categorisation and Classification Method [16].

#### 7.2.2.3.2 Environment, Security and Safeguards Classification

No environment, security, or safeguards classification is assigned at RD7/DRP1.

#### 7.2.2.3.3 Seismic performance classification

The RPCS [JSA] is to be classified in accordance with the RR SMR Seismic Performance Classification Method [17].

## 7.2.3 Description

The RPCS [JSA] comprises of the following sub-systems:

- The Reactor Control System [JSA10], which provides the duty level, plant process control and monitoring during normal operation of the primary reactor systems and associated heat exchangers



- The Reactor Limitation & Preventative Protection System [JSA20], which detects deviations from the plant's normal operating conditions, and provides preventative safety measures to restore the plant's state to within normal operating limits
- The Control Rod Control System [JSA30], which directly provides drive power to the Control Rod Drive Mechanisms (CRDMs), it interfaces with other Reactor Plant Control subsystems to execute rod movement commands, and provides continuous rod position indication. Ongoing design work may result in the Rod position indications requiring a higher classification and as a result will be separated from the lower classified parts of the [JSA30]
- The Nuclear Heating, Ventilation and Air Conditioning (HVAC) Supervisory Control System [JSA40], which acts as a supervisory controller for the distributed local Reactor Island HVAC controllers with a commensurate or lower safety classification to JSA40. The category B or category A HVAC functions will not be implemented in this system, but inside RPS and DPS, or in systems based on the same platforms as RPS and DPS respectively.

A detailed description of the RPCS [JSA] and associated subsystems is provided in the System Design Description document [18].

## 7.2.4 Materials

N/A.

## 7.2.5 Interfaces

Interfaces for the Reactor Plant Control System [JSA] are identified and managed within the requirements specification module for the respective system in the RR SMR requirements management database.

Measurements for the RCS [JSA10] and RLPPS [JSA20] are only shared “downwards” from the RLPPS [JSA20] in DiD level 2 to the RCS [JSA10] in DiD level 1 to prevent fault propagation from the RCS [JSA10] inhibiting the functionality of the RLPPS [JSA20].

Measurements from the RPS [JRA] or DPS [JQA] to the RLPPS [JSA20] (and by extension the RCS [JSA10]) is acceptable in limited cases where analysis shows that the measured parameters are not used in both systems to mitigate the same fault or where the same signal could cause the RCS to initiate a fault mitigated by the RPS.

## 7.2.6 System and Equipment Operation

The RR SMR Power Station Operating Philosophy [19] provides the overarching information on how the plant and operator maintain control of key functions across the six defined operating modes, including the operating principles, required actions, means for transitioning between the operating modes, and relevant safety systems for each mode.

## 7.2.7 Instrumentation and control

N/A.



## 7.2.8 Monitoring, Inspection, Testing and Maintenance

The maintenance tasks and procedures, specific to the RPCS [JSA] environment and operating context are still being developed at RD7/DRP1 in line with the high-level C&I Strategy [20].

## 7.2.9 Radiological Aspects

The RPCS [JSA] provides a supporting function to various safety measures. It does not propose a direct radiation hazard. No specific radiation assessments required for the RPCS [JSA].

## 7.2.10 Performance and Safety Evaluation

The outline approach to system verification is presented in the Approach to Verification of C&I Systems report [21]. It sets out how the RPCS [JSA] will be verified to meet its safety categorised functional requirements. Additionally, the Approach to Integration and Validation of C&I Systems document [22] proposes a series of integration and validation activities to be conducted following C&I component manufacture.

Key RPCMS [JS] design decisions made with respect to ensuring overall risks are reduced to ALARP include the selection of the level of redundancy. The RPCS will be implemented using an N+1 redundancy which provides the optimised position with respect to achieving reliability targets and minimising the demand on the protection C&I systems.



## 7.3 Reactor Protection System

---

### 7.3.1 System and Equipment Functions

The RPS [JRA] comprises of two main sub-systems, RPS 1 [JRA10] and RPS 2 [JRA20], which fulfil two primary roles:

- Secondary means of implementing all safety category A functions (alongside the DPS [JQA] at DiD level 3, fulfilled by RPS 1 [JRA10])
- Implementation of DiD level 3 safety category B functions, fulfilled by RPS 2 [JRA20]

### 7.3.2 Design Bases

#### 7.3.2.1 Functional requirements

The RPS [JRA] facilitates delivery of CoR, CoFT, CoRM during fault and abnormal conditions. Safety categorised functional requirements specified for the RPS [JRA] based on the HLSFs they deliver, including the applicable plant states, are presented in Table 7.3-1. The functional requirements in Table 7.3-1 correspond to the allocated protective and preventative functions from the Engineering Schedule [7].

**Table 7.3-1: RPS [JRA] Safety Categorised Functional Requirements**

Functional Requirement	Plant State(s)	Safety Category
When demanded, the [JRA] System shall Initiate Scram [JD01]	DBC-3i- DBC-4	A
When demanded, the [JRA] System shall Initiate high pressure ADS	DBC-3i- DBC-4	A
When demanded, the [JRA] System shall Initiate low pressure ADS	DBC-3i- DBC-4	A
When demanded, the [JRA] System shall Initiate steam and feed isolation	DBC-3i- DBC-4	A
When demanded, the [JRA] System shall Initiate Containment Isolation (ECC)	DBC-3i- DBC-4	A
When demanded, the [JRA] System shall provide Low Temperature Over Pressure (LTOP) Isolation Interlock.	DBC-3i- DBC-4	A
When demanded, the [JRA] System shall provide Cold Shutdown Cooling System (CSCS) Isolation Interlock	DBC-3i- DBC-4	A
When demanded, the [JRA] System shall Initiate Containment Isolation (LOCA)	DBC-3i- DBC-4	B
When demanded, the [JRA] System shall Initiate Alternative Shutdown Function Phase 1	DBC-3i- DBC-4	B



When demanded, the [JRA] System shall initiate Alternative Shutdown Function Phase 2	DBC-3i- DBC-4	B
When demanded, the [JRA] System shall Initiate high pressure injection system	DBC-3i- DBC-4	B
When demanded, the [JRA] System shall Initiate passive steam condensing cooling	DBC-3i- DBC-4	B
When demanded, the [JRA] System shall Initiate Reactor Coolant System [JE] connecting systems isolation	DBC-3i- DBC-4	B
When demanded, the [JRA] System shall Initiate Chemistry and Volume Control System [KB] Isolation	DBC-3i- DBC-4	B
When demanded, the [JRA] System shall Initiate atmospheric steam dump over pressure protection	DBC-3i- DBC-4	B
When demanded, the [JRA] System shall Initiate isolation of atmospheric steam dump	DBC-3i- DBC-4	B
When demanded, the [JRA] System shall initiate isolation of high pressure injection system	DBC-3i- DBC-4	B
When demanded, the [JRA] System shall initiate isolation of steam generator feed	DBC-3i- DBC-4	B
When demanded, the [JRA] System shall initiate steam generator tube rupture response	DBC-3i- DBC-4	B
When demanded, the [JRA] System shall Initiate low pressure injection system	DBC-3i- DBC-4	B
When demanded, the [JRA] System shall initiate single steam generator isolation	DBC-3i- DBC-4	B
When demanded, the [JRA] System shall Initiate Spent Fuel Pool Isolation	DBC-3i- DBC-4	B
When demanded, the [JRA] System shall Recover Component Cooling System (CCS) & Essential Service Water System (ESWS).	DBC-3i- DBC-4	B
When demanded, the [JRA] System shall start Standby AC Power	DBC-3i- DBC-4	B
When demanded, the [JRA] System shall Initiate class 2 HVAC	DBC-3i- DBC-4	B

The functional requirements in Table 7.3-1 correspond to the allocated protective and preventative measures from the Engineering Schedule [7]. The safety categorised functional requirements for the RPS [JRA], and associated non-functional performance requirements, are listed in the RR SMR requirements management database RPS [JRA] requirements specification module.

### 7.3.2.2 Non-functional requirements

The non-functional system requirements for the RPS [JRA] are listed in the Reactor Island Control & Protection System [JY] module in the RR SMR requirements management database, based on the design rules listed in section 7.1.2.2. The allocated requirements allocated to the RPS are then flown



down to the RPS [JRA] requirements specification module, which provides a full set of non-functional requirements for the system.

### 7.3.2.3 E3S classification

#### 7.3.2.3.1 Safety Classification

The RPS [JRA] provides a secondary means of fulfilling a category A safety function and provides the principal means of fulfilling a safety category B safety function, and in accordance with the E3S Categorisation and Classification methodology outlined in E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules, [8], is classified as safety class 2. Further work will be performed after RD7/DRP1 to determine whether this classification is flowed down to all RPS subsystems or whether a lower classification can be assigned to some parts of the RPS that for example only deliver category C or no nuclear safety functions.

#### 7.3.2.3.2 Environment, Security and Safeguards Classification

No environment, security, or safeguards classification is assigned at RD7/DRP1.

#### 7.3.2.3.3 Seismic performance classification

In accordance with the SMR Seismic Performance Classification Method [17] all safety class 1 and safety class 2 SSCs shall be classified as Seismic Performance Class 1 (SPC1). Therefore, the RPS, being a class 2 system is assumed to be classified as SPC1.

### 7.3.3 Description

The RPS [JRA] comprises of the following sub-systems

- Reactor Protection System 1 (RPS1) [JRA10], which performs category A function duplicated in the DPS with a set of diverse initiating parameters wherever possible
- Reactor Protection System 2 (RPS2) [JRA20], which incorporates all the category B C&I safety functions across the plant
- Neutron flux monitoring system (NFMS) [JRA30], which processes the output from neutron detectors and provides derived trip parameters to the RPS 1 and RPS 2 subsystems for trip determination on the SCRAM and ASF functions
- Reactor trip breakers (RTB) [JRA40], which cuts power to the Control Rod Drive Mechanisms (CRDM) in response to the voting function initiating SCRAM
- Priority Logic System (PLS) [JRA50], which prioritises functions, translate function demands to actuator commands and prioritises actuation
- RPS Monitoring System (RPSMS) [JRA60], which provides monitoring and maintenance functionality for the RPS and acts as an interface to the RPS Panels and Displays subsystem
- Reactor protection system panels and displays (RPSPD) [JRA90], which provides the interface to operators in the MCR and SCR for displaying RPS information, alarms and for processing inputs for manual protection functions and other manual operations, such as bypassing parameter votes or whole divisions.



A detailed description of the RPS [JRA] and associated subsystems is provided in the System Design Description document [23].

### 7.3.4 Materials

N/A.

### 7.3.5 Interfaces

Interfaces for the Reactor Protection System [JRA] are identified and managed within the requirements specification module for the system in the RR SMR requirements management database and a diagram of the interfaces is shown in the System Design Description document [23].

### 7.3.6 System and Equipment Operation

The RR SMR Power Station Operating Philosophy [19] provides the overarching information on how the plant and operator maintain control of key functions across the six defined operating modes, including the operating principles, required actions, means for transitioning between the operating modes, and relevant safety systems for each mode. The operating philosophy for the RPS [JRA] is to be developed. It is currently assumed that some or all of the RPS will be required to be operational in all modes of operation because safety functions delivered by the RPS are claimed in all modes of operation.

#### 7.3.6.1 Degraded modes

The RPS is expected to remain operational and fulfil its safety function if one division has been taken offline for maintenance. In this configuration, each instance of 2 out of 3 (2oo3) voting is currently assumed to change to 2 out of 2 (2oo2) to minimise the risk of spurious actuation. Further analysis is required to validate that this design decision is acceptable from a pfd perspective. A review will be carried out once the design and PSA have been developed further post RD7/DRP1.

When a division of the RPS is out of operation due to maintenance, operators in the control room will be notified of this condition so that they can assure compliance to the plant technical specifications.

#### 7.3.6.2 Faulted Operations

The concept of fail-safe design will be incorporated, as appropriate, into the design of the RPS. This includes ensuring the system is designed to go to a safe condition for its most probable known failure modes.

### 7.3.7 Instrumentation and control

N/A.

### 7.3.8 Monitoring, Inspection, Testing and Maintenance

The RPS EMIT strategy is to be developed in line with the high-level C&I EMIT Strategy. A number of assumptions regarding EMIT non-functional and functional requirements were derived from RGP



and standards to inform the design of the RPS Monitoring System [JRA60] in particular. A subset of these is provided below:

- During any EMIT activity, the RPS shall remain compliant to its design basis safety case.
- The RPS shall accommodate functional testing of the full safety function whilst the plant is online and the RPS division is in maintenance mode.
- The RPS shall monitor its own hardware and inputs from interfacing hardware that could affect the RPS safety function.
- Surveillance tests shall confirm that the RPS safety features will operate as per their design intent when commanded.
- The RPS shall have maintenance bypasses to prevent functions from activating spuriously during EMIT activities whilst the SMR plant is online.
- The RPS should have a reset functionality that can be executed upon operator command. Safeguards will be put in place so that it will only be possible to reset one division at a time.
- The RPS shall provide diagnostic information to maintenance technicians via the maintenance interface when it is in maintenance mode.
- The RPS shall provide fault code store access to maintenance technicians via the maintenance interface when it is in maintenance mode.
- The RPS shall record historical data for all safety functions in a format that can be reviewed by an operator.
- The RPS should accommodate a software update, including set point values, on any one of its divisions whilst that division is in maintenance mode and the plant is at power.

### 7.3.9 Radiological Aspects

The Reactor Protection System [JRA] provides a supporting function to various safety measures. The system in itself does not pose a radiation hazard. No specific radiation assessments are required for the Reactor Protection System [JRA].

### 7.3.10 Performance and Safety Evaluation

The outline approach to system verification is presented in the Approach to Verification of C&I Systems report [21]. It sets out how the RPS [JRA] will be verified to meet its safety categorised functional requirements. Additionally, the Approach to Integration and Validation of C&I Systems document [22] proposes a series of integration and validation activities to be conducted following C&I component manufacture.

Key design and performance assessments that underpin the design of the Reactor Protection System [JRA] and demonstrate how the definition meets the non-functional performance requirements associated with the key system functions are still in development.

## 7.4 Diverse Protection System

### 7.4.1 System and Equipment Functions

The DPS [JQA] is a class 1 protection system, the primary function of which is to provide the Reactor Island Control and Protection [JY] implementation of the DiD level 3, category A safety functions, by diverse means to the class 2 RPS [JRA].

### 7.4.2 Design Bases

#### 7.4.2.1 Functional requirements

The DPS [JQA] facilitates delivery of CoR, CoFT, CoRM during fault and abnormal conditions. Safety categorised functional requirements specified for the DPS [JQA] based on the HLSFs they deliver, including the applicable plant states, are presented Table 7.4-1.

**Table 7.4-1: DPS [JQA] Safety Categorised Functional Requirements**

Safety Functional Requirement	Plant State(s)	Safety Category
When demanded, the [JQA] System shall Initiate Diverse Scram [JD01]	DBC-3i- DBC-4	A
When demanded, the [JQA] System shall Initiate diverse high pressure Automatic Depressurisation System (ADS)	DBC-3i- DBC-4	A
When demanded, the [JQA] System shall Initiate diverse low pressure ADS	DBC-3i- DBC-4	A
When demanded, the [JQA] System shall Initiate Diverse Steam and Feed Isolation	DBC-3i- DBC-4	A
When demanded, the [JQA] System shall Initiate Diverse Containment Isolation (ECC)	DBC-3i- DBC-4	A
When demanded, the [JQA] System shall provide Diverse Low Temperature Over Pressure (LTOP) Isolation Interlock	DBC-3i- DBC-4	A
When demanded, the [JQA] System shall provide Diverse CSCS Isolation Interlock	DBC-3i- DBC-4	A
When demanded, the [JQA] System shall initiate Diverse Spent Fuel Pool Isolation	DBC-3i- DBC-4	A
When demanded, the [JQA] System shall Initiate class 1 HVAC	DBC-3i- DBC-4	A

The functional requirements in Table 7.4-1 correspond to the allocated protective and preventative measured from the Engineering Schedule [7]. The safety categorised functional requirements for the DPS [JQA], and associated non-functional performance requirements, are listed in the RR SMR requirements management database DPS [JQA] requirements specification module.



#### 7.4.2.2 Non-functional requirements

The non-functional system requirements for the DPS [JQA] are listed in the Reactor Island Control & Protection System [JY] module of the RR SMR requirements management database, based on the design rules listed in section 7.1.2.2. The allocated requirements allocated to the DPS are then flown down to the DPS [JQA] requirements specification module, which provides a full set of non-functional requirements for the system.

#### 7.4.2.3 E3S classification

##### 7.4.2.3.1 Safety classification

The DPS [JQA] has been assigned a class 1 safety classification where the sub-systems provide the primary means to perform category A safety functions. These sub-systems are:

- Diverse Logic Solver (DLS) [JQA10]
- Diverse Neutron Flux Monitoring System (DNFMS) [JQA30]
- Diverse Reactor Trip Breakers (DRTB) [JQA40]
- Diverse Priority Logic System (DPLS) [JQA50]
- DPS Panels and Displays (DPSPD) [JQA90]

The DPS Monitoring System (DPSMS) [JQA60] sub-system is a monitoring system only, and does not perform plant safety functions, and has therefore been assigned a class 2 safety classification.

##### 7.4.2.3.2 Environment, Security and Safeguards Classification

No environment, security, or safeguards classification is assigned at RD7/DRP1.

##### 7.4.2.3.3 Seismic performance classification

In accordance with the RR SMR Seismic Performance Classification Method [17], all safety class 1 and safety class 2 SSCs shall be classified as SPC1. Therefore, the DPS [JQA] is classified as SPC1.

### 7.4.3 Description

The DPS [JQA] comprises of the following sub-systems:

- The DLS [JQA10], which is a class 1, non-programmable sub-system that provides the logic solving and voting functions of the DPS [JQA] and is implemented in four redundant, independent divisions. The DLS [JQA10] interfaces with sensors, the DNFMS [JQA30], and performs signal conditioning. The DLS [JQA10] provides trip commands to the DRTB [JQA40] and DPLS [JQA50]. The DLS [JQA10] provides trip status information to the DPSMS [JQA60] and DPSPD [JQA90] in the MCR and SCR.
- The DNFMS [JQA30], which is a class 1, non-programmable sub-system that interfaces with neutron flux detectors and performs signal conditioning to allow the DPS [JQA] to interpret neutron flux over the full range of reactor power operating levels. The DNFMS [JQA30] is implemented in four redundant, independent divisions.



- The DRTB [JQA40] is a class 1, non-programmable sub-system that actuates the automatic Scram function via trip breakers and is implemented in four redundant, independent divisions.
- The DPLS [JQA50], which handles the priority of demands for shared actuators. The DPLS [JQA50] is implemented at actuator level via Priority Logic Units (PLUs), each PLU is assigned to one actuator. The DPLS [JQA50] and the PLUs contained within it are class 1.
- The DPSMS [JQA60], which is a class 2, programmable sub-system which monitors the DPS [JQA] and its sub-systems and displays this information in the MCR and SCR. It is implemented in two redundant, independent divisions.
- The DPSPD [JQA90], which is a class 1, non-programmable sub-system that provides an operator interface for the DPS [JQA] in the MCR and SCR, and is implemented in four redundant, independent divisions.

A detailed description of the DPS [JQA] and associated subsystems is provided in the System Design Description document [24].

#### 7.4.4 Materials

N/A.

#### 7.4.5 Interfaces

The interfaces of the DPS [JQA] architecture can be seen in DPS [JQA] architecture drawing [25]. All interfaces for the DPS [JQA] are identified and managed within the DPS [JQA] requirements specification module in the RR SMR requirements management database. The complete description of DPS interfaces will be presented in Version 3 of the generic E3S case.

#### 7.4.6 System and Equipment Operation

The RR SMR Power Station Operating Philosophy [19] provides the overarching information on how the plant and operator maintain control of key functions across the six defined operating modes, including the operating principles, required actions, means for transitioning between the operating modes, and relevant safety systems for each mode.

The operating philosophy and a full analysis of the system operation in all modes of operation are to be developed and will be presented in Version 3 of the generic E3S Case. It is expected that some, or all, of the DPS [JQA] should be required to be operational in all modes of operation. Safety functions delivered by the DPS [JQA] are claimed in all modes of operation.

The DPS [JQA] is expected to remain operational and to fulfil its safety function, with the SFC met, if one division has been taken ‘offline’ for maintenance. It is assumed that when a division of the DPS [JQA] is ‘offline’ due to maintenance, operators in the control room shall be notified of this condition so that they can ensure compliance to the plant technical specifications.

For faulted operations, the concept of fail-safe design will be incorporated, as appropriate, into the design of the DPS [JQA]. This includes ensuring that the system is designed to fail in a safe condition for the known, and most probable, failure modes, and to meet the SFC requirement.



## 7.4.7 Instrumentation and control

N/A.

## 7.4.8 Monitoring, Inspection, Testing and Maintenance

The maintenance tasks and procedures, specific to the DPS[JQA] environment and operating context are still being developed in line with the high-level C&I Strategy [20].

## 7.4.9 Radiological Aspects

The DPS [JQA] does not pose a radiation hazard. No specific DPS [JQA] radiation assessments are required.

## 7.4.10 Performance and Safety Evaluation

The outline approach to system verification is presented in the Approach to Verification of C&I Systems report [21]. It sets out how the DPS [JQA] will be verified to meet its safety categorised functional requirements. Additionally, the Approach to Integration and Validation of C&I Systems document [22] proposes a series of integration and validation activities to be conducted following C&I component manufacture.



## 7.5 Accident Management System

---

### 7.5.1 System and Equipment Functions

The primary function of the AMS [JRQ] is to support on-site staff in making decisions for the management of Design Basis Accidents (DBAs), DECs, and severe accidents. The role of the AMS [JRQ] is to provide monitoring instrumentation and systems for preventive and mitigative accident management.

### 7.5.2 Design Bases

#### 7.5.2.1 Functional requirements

The AMS [JRQ] facilitates the delivery of CoR, CoFT and CoRE during accident conditions. At RD7/DRP1, no functional requirements have been allocated to the AMS [JRQ] from plant operations, instead the requirements for the AMS [JRQ] are based on BS IEC 63147:2017 [14] and guidance for the application of IEC 63147:2017 [15].

The safety categorised functional requirements for the AMS [JRQ] and associated non-functional performance requirements, are listed in the RR SMR requirements management database AMS [JRQ] requirements specification module.

#### 7.5.2.2 Non-functional requirements

The non-functional system requirements for the AMS [JRQ] are listed in the Reactor Island Control & Protection System [JY] module of the RR SMR requirements management database, based on the design rules listed in section 7.1.2.2. The allocated requirements allocated to the AMS are then flown down to the AMS [JRQ] requirements specification module, which provides a full set of non-functional requirements for the system.

#### 7.5.2.3 E3S classification

##### 7.5.2.3.1 Safety classification

The PAMS [JRQ10] safety class is dependent on the types of variables to be monitored as informed by IEC 63147:2017 guidance [15], while the SAMS [JRQ20] is classified as class 3, because it is expected to only fulfil category C functions.

**Table 7.5-1: Allocation of Safety Class to PAMS [JRQ10] Variables**

Variable type Definition based on IEC 63147:2017 [14]	Short Definition based on IEC 63147:2017 [14]	IEC 61226 [26] safety class
A	Safety functions for which there is no automatic control	1, 2 or 3, depending on safety category
B	Primary safety functions (reactivity control / core cooling / reactor coolant system integrity / containment integrity)	2



Variable type Definition based on IEC 63147:2017 [14]	Short Definition based on IEC 63147:2017 [14]	IEC 61226 [26] safety class
C	Fission product barriers (fuel cladding / reactor coolant system pressure boundary / containment pressure boundary)	2
D	Performance of safety systems and auxiliary supporting features	2 or 3, depending on safety category
E	Magnitude of the release of radioactive materials and continually assessing such releases	3
F	Fuel damage and the effects of fuel damage	3

It is not expected that any type A variables will be needed for the RR SMR project.

### 7.5.2.3.2 Environment, Security and Safeguards Classification

No environment, security, or safeguards classification is assigned at RD7/DRP1.

### 7.5.2.3.3 Seismic performance classification

The AMS [JRQ] is to be classified in accordance with the RR SMR Seismic Performance Classification Method [17].

## 7.5.3 Description

The AMS [JRQ] comprises of the following sub-systems:

- PAMS [JRQ10], which provides monitoring instrumentation and systems for preventive and mitigative accident management during DBA
- SAMS [JRQ20], which provides monitoring instrumentation and systems to allow initiation of severe accident safety systems for mitigative accident management during DECs and severe accidents in alignment with the severe accident management strategy [27]

A detailed description of the AMS [JRQ] and associated subsystems is provided in the System Design Description document [28].

## 7.5.4 Materials

N/A.

## 7.5.5 Interfaces

Interfaces for the AMS [JRQ] are to be identified and managed within the AMS [JRQ] requirements specification module in the RR SMR requirements management database. The complete description of AMS interfaces will be presented in Version 3 of the generic E3S case.



## 7.5.6 System and Equipment Operation

The RR SMR Power Station Operating Philosophy [19] provides the overarching information on how the plant and operator maintain control of key functions across the six defined operating modes, including the operating principles, required actions, means for transitioning between the operating modes, and relevant safety systems for each mode.

The operating philosophy and a full analysis of the AMS [JRQ] operation in all modes of operation are to be developed.

## 7.5.7 Instrumentation and control

N/A.

## 7.5.8 Monitoring, Inspection, Testing and Maintenance

The maintenance tasks and procedures, specific to the AMS [JRQ] environment and operating context are still being developed in line with the high-level C&I Strategy [20].

## 7.5.9 Radiological Aspects

The AMS [JRQ] provides a supporting function to various safety measures. It in itself does not pose a radiation hazard. No specific radiation assessments are required for the AMS [JRQ].

## 7.5.10 Performance and Safety Evaluation

The outline approach to system verification is presented in the Approach to Verification of C&I Systems report [21]. It sets out how the AMS [JRQ] will be verified to meet its safety categorised functional requirements. Additionally, the Approach to Integration and Validation of C&I Systems document [22] proposes a series of integration and validation activities to be conducted following C&I component manufacture.

## 7.6 Reactor Plant Monitoring System

---

### 7.6.1 System and Equipment Functions

The RPMS [JSS] is a subsystem of the RPCMS [JS].

The Reactor Plant Monitoring System [JSS] is a collection of standalone, specialised monitoring and analysis sub-systems used on the Reactor Island. These systems will, either directly or indirectly, provide data to assist operation and maintenance staff to enable data driven trouble shooting and maintenance planning.

### 7.6.2 Design Bases

#### 7.6.2.1 Functional requirements

No safety functional requirements have been identified for the RPMS [JSS] at RD7/DRP1.

#### 7.6.2.2 Non-functional requirements

The non-functional requirements are consolidated in the Reactor Island Control and Protection Systems [JY] module of the RR SMR requirements management database, which are based on the design rules listed in section 7.1.2.2, and are then allocated where appropriate to the Reactor Plant Monitoring System [JSS] module. Some non-functional requirements will be allocated unaltered, while others will require further decomposition, potentially on analysis, such as cross C&I system diversity and independence requirements.

#### 7.6.2.3 E3S classification

##### 7.6.2.3.1 Safety classification

At this stage it is expected that the highest safety category of functions provided by the RPMS [JSS] will be ‘not categorised’.

##### 7.6.2.3.2 Environment, Security and Safeguards Classification

No environment, security, or safeguards classification is assigned at RD7/DRP1.

##### 7.6.2.3.3 Seismic performance classification

The RPMS [JSS] is to be classified in accordance with the RR SMR Seismic Performance Classification Method [17].

### 7.6.3 Description

The RPMS [JSS] comprises the following sub-systems:

- In-core Flux monitoring system [JSS10], which provide indications to the operator of the local neutron flux at the in-core detector positions (e.g., a 3D flux map), as well as functions



calculating axial and radial offsets. Ongoing design work may result in this system performing higher classified functions and as a result becoming part of a protection system.

- Loose-Parts Detection system [JSS20], which detect loose parts (bolts, loose materials, etc.) in real time to provide operation and maintenance staff with advanced warning of potential consequential plant failures
- Rotary Equipment Vibration Monitoring and Diagnostics systems [JSS30], which provide a rotary equipment analytic system used to identify progressive degradation for predictive maintenance purposes. Includes, but not limited to, pump vibration, pump motor winding temperature and gasket leakage monitoring.
- Neutron Noise Monitoring system [JSS50], which provides an analytical tool that utilises neutron sensing to detect excessive core barrel vibrations or flow anomalies within the Reactor Pressure Vessel (RPV)
- Primary Circuit Leak Detection system [JSS60], which detects early signs of potential leaks within the primary circuit. Achieved using, but not limited to, a combination of humidity, ambient temperature, vibration, and acoustic sensor.
- Valve Monitoring system [JSS70], which provides continuous monitoring of valve stroking performance, excessive valve vibration and valve seat leakage to identify progressive degradation for predictive maintenance purposes
- Seismic Monitoring system [JSS80], which continuously monitors, captures, and analyses seismic event data and provides alarms to operators. This system is independent to any seismic monitoring performed as part of an automated safety shutdown systems.
- Reactor Island Sampling system [JSS90], which provides signal processing capabilities for a variety of the online water analysers (dissolved O<sub>2</sub>, pH, Boron, conductivity etc) that make up the nuclear plant's chemistry sampling system. The system provides alarms to the operator indicating undesirable conditions and independent to any chemistry monitoring performed as part of an automated safety shutdown systems.

A detailed description of the RPMS [JSS] and associated subsystems is provided in the System Design Description document [29].

## 7.6.4 Materials

N/A.

## 7.6.5 Interfaces

Interfaces for the RPMS [JSS] are identified and managed within the requirements specification module for the system in the RR SMR requirements management database. The complete description of RPMS interfaces will be presented in future revision of the generic E3S case.

## 7.6.6 System and Equipment Operation

The RR SMR Power Station Operating Philosophy [19] provides the overarching information on how the plant and operator maintain control of key functions across the six defined operating modes,



including the operating principles, required actions, means for transitioning between the operating modes, and relevant safety systems for each mode.

## 7.6.7 Instrumentation and control

N/A.

## 7.6.8 Monitoring, Inspection, Testing and Maintenance

The maintenance tasks and procedures, specific to the RPMS [JSS] environment and operating context are still being developed in line with the high-level C&I Strategy [20].

## 7.6.9 Radiological Aspect

The Reactor Plant Monitoring System [JSS] provides data collection and analysis for the Reactor Island. It in itself does not pose a radiation hazard. No specific radiation assessments required for the Reactor Plant Monitoring System [JSS].

## 7.6.10 Performance and Safety Evaluation

The outline approach to system verification is presented in the Approach to Verification of C&I Systems report [21]. It sets out how the RPMS [JSS] will be verified to meet its safety categorised functional requirements. Additionally, the Approach to Integration and Validation of C&I Systems document [22] proposes a series of integration and validation activities to be conducted following C&I component manufacture.

Key RPMS [JSS] design decisions made with respect to ensuring overall risks are reduced to ALARP include the selection of the level of redundancy. The RPMS will be implemented without redundancy because it is not required for nuclear safety.



## 7.7 Other C&I Systems

### 7.7.1 Data Processing and Control System

The primary function of the Data Processing and Control System (DPCS) is to provide means for duty control and operation of the RR SMR nuclear power plant by operators in the control rooms. The DPCS will provide the Operator with an up to date and comprehensive view of the overall status of the SMR for duty and all modes of the reactor.

The DPCS is currently assessed as class 3 system, based on providing functions as part of the duty control function and preventive measures.

The systems that form part of the DPCS are:

- DPCS - Main Controller
- Automation System
- Diagnostic System
- Engineering Systems – DPCS
- Data Transfer Network Systems
- Reactor Plant Control and Monitoring Systems
- Fuel Route C&I
- Radioactive Waste Management System C&I

The descriptions of these systems are covered in the subsequent sub-sections, except the RPCMS covered in sections 7.2 and 0.

All the functions required within the DPCS can be implemented within a class 3 system architecture, so for the use of common components and systems, the control nodes on the DPCS including RPCMS, will use the same technology that will be qualified for the DPCS. This provides significant opportunities to make use of Commercial off the Shelf (COTS) solutions, which can be sourced more widely in the supply chain. It is noted that some parts of the DPCS will probably require dedicated platforms (e.g. the Control Rod Control System).

#### 7.7.1.1 Automation System

The Automation System will be a sub-system of the station DPCS. It is required to automate the power station process, at the overarching level, in coordination with all its islands. It interfaces with all the island automation systems to gather and display operational data and to provide those systems with supervisory control.

The Automation System will chiefly consist of a set of automation controllers that will provide inter-island automation to the SMR process, in a central strategic location. These controllers will



communicate with the rest of the power station automation, providing data to and from the island control systems.

### 7.7.1.2 Diagnostic System

The primary function of the Diagnostic System is to provide diagnostics for the power station processes. The system will interface to machinery diagnostic systems, within each island, and present an overarching set of diagnostics to the operators and maintainers in central locations, such as the control rooms.

The system will chiefly consist of a set of servers that will provide diagnostics to HMIs in each control room, and in other strategic maintenance locations, as required.

### 7.7.1.3 Engineering System - DPCS

The primary function of the Engineering System - DPCS is to provide a maintenance and engineers facility to the DPCS. It is to provide an engineers and maintainers facility for the equipment that forms the DPCS, such as servers, controllers, HMIs, and network equipment.

Under strict procedural control, this system will allow alterations and revisions to the software and firmware of each of the components within the DPCS including the distributed controller nodes. It will also be able to interrogate each sub-system to understand its system health and software revisions. It will be the means to download and upload software for all the overarching systems.

### 7.7.1.4 Data Transfer Network Systems

The primary function of Data Transfer Network Systems is to provide the network medium for the control and management systems. It will be made up of routers, switches, and other network equipment.

The systems are sub-divided into two sub-systems; Data Transfer – Terminal Network and Data Transfer – Automation Network. These systems will have a number of dedicated networks that will ensure the safe and efficient operation of the nuclear facility by allowing operators and engineers to remotely access, monitor, and manage essential processes and equipment.

### 7.7.1.5 Fuel Route C&I

The high-level role of the Fuel Route C&I System is to provide control, protection and monitoring of the Fuel Route SSCs. Applicable SSCs fall ‘mostly’ under the ‘Handling of Nuclear Equipment’ system; this includes several fuel and mechanical handling systems in addition to the pools and their respective cooling, purification, and supply systems.

Key functions / functional objectives of the Fuel Route C&I System are as follows:

- Monitor the Fuel Route SSCs, collate/pass the necessary data to the associated external systems and provide the interface between the plant and the DPCS
- Protect the Fuel Route SSCs through a system of permits and interlocks and implement safety measures as required by the RR SMR Fault Schedule
- Support any Environmental, Security or Safeguards functions as required by the respective analyses



- Provide any supervisory or additional control functions which cannot be implemented locally in the Fuel Route SSCs
- Store data/properties (including location) of all Fuel Assemblies, New-Fuel Shipping Containers and Spent Fuel Casks (for inventory tracking)

The C&I safety functions required from Fuel Route C&I system and its subsystems are expected to be no greater than safety category C, commensurate with a safety class 3 system.

It is anticipated that some Fuel Route SSCs will utilise PLCs and will be connected to the DPCS via a networked connection; hardwiring may also be used for some systems and signals.

It is anticipated that some Fuel Route SSCs will utilise local HMIs / Operator Panels connected to their local PLC. This is separate to any HMI functionality provided by the Distributed Control System.

### 7.7.1.6 Radioactive Waste Management System C&I

The Radioactive Waste Management System (RWMS) C&I is a duty control system that provides control and monitoring of solid, liquid, and gaseous radioactive waste processes on the RR SMR plant. It performs continuous and batch-based process control of radioactive waste systems, including automatic, semi-automatic and manual configuration of radioactive waste process plant. It monitors a range of process parameters and provides control through actuation of process equipment. The RWMS C&I is currently designated as a class 3 C&I system which carries out some category C safety functions at DiD 1.

The process and system indications, warnings and alarms are provided to the operator from the RWMS C&I. The RWMS C&I also provides a supervisory role for the control and monitoring of package radioactive waste systems (e.g. skid-mounted or mobile systems) that include their own dedicated control systems.

Operator control and monitoring of the RWMS C&I will be provided from remote and local control centres. The RWMS C&I equipment will be primarily located adjacent to the radioactive waste process systems in the RR SMR Auxiliary Block. Components associated with the Reactor Island Drainage System may be located across various areas within the Reactor Island.

The RWMS C&I comprises three individual C&I Systems:

- Liquid Radioactive Waste Management System C&I
- Gaseous Radioactive Waste Management System C&I
- Solid Radioactive Waste Management System C&I

The RWMS control systems shall be implemented as a class 3 system making use of COTS solutions.

### 7.7.2 Process Monitoring System

The Process Monitoring System consists of the following sub-systems:

- Fire Alarm System: This system will typically consist of a main fire alarm panel (or panels) connected to smoke, flame and thermal sensors, Break Glass Units / Manual Call Points



(MCPs), Tonal / Voice Sounders and Sirens, Flashers and Beacons, Extinguishing Systems and Fireman's Control Panels.

- Gas Warning System: This system will typically consist of a main controller connected to gas detectors, Manual Call Points (MCPs), Tonal / Voice Sounders and Sirens, Flashers, and Beacons. These tend to be COTS products.
- Video Monitoring System: This system typically consists of several cameras, usually networked together, and connected to a software package or packages, hosted on a server. This system may require to be interfaced with the security surveillance system.
- Alarm System (Acoustic/Optical): These systems typically consist of a main alarm control panel (or panels) connected to audio-visual alarm beacons, sounders and sirens, and Manual Call Points (MCPs).
- Emission and Immission Monitoring System: This can be considered in two main categories, radiological emissions and conventional environmental emissions.
- Meteorological Reporting System: This system is to monitor the prevailing weather and forecast future weather to assist operational planning and response.

### **7.7.3 Feedwater, Steam and Condensate Control and Protection System**

The primary function of the Feedwater, Steam and Condensate Control and Protection System is to control and protect all the equipment contained in the Feedwater, Steam and Condensate System. The system comprises of the following subsystems:

- Feedwater Control and Protection System – with primary function to control and protect all the equipment contained within the feedwater system.
- Steam System Control and Protection System – with primary function to control and protect all the equipment contained within the steam system.
- Condensate Control and Protection System – with primary function to control and protect all the equipment contained within the condensate system.
- Condensate Polishing Control and Protection – with primary function to control and protect all the equipment contained within the condensate polishing system.
- Auxiliary Feedwater Control and Protection System – with primary function to control and protect all the equipment contained within the auxiliary feedwater system.

The Feedwater, Steam and Condensate Control and Protection System, and all its subsystems are currently given an overall maximum preliminary safety classification of class 3. The system platform will be based around a DPCS, with certain systems using other dedicated controllers.

The Feedwater, Steam and Condensate Control and Protection System Design Description document provides further details on the design [30].



## 7.7.4 Turbine Island Control and Protection System

The primary function of the Turbine Island Control and Protection System is to control and protect all the equipment contained within the Turbine hall. The system comprises of the following subsystems:

- Steam Turbine System Control and Protection System – with primary function to control and protect all the equipment contained within the main steam turbine system
- Generator System Control and Protection System – with primary function to control and protect all the equipment contained within the main generator system
- Generator Transmission Main Connection System – with primary function to control and protect all the equipment contained within the main generator transmission main connection system

The Turbine Island Control & Protection System, and all its subsystems are currently given an overall maximum preliminary safety classification of class 3. The system platform will be based around a DPCS, with certain systems using other dedicated controllers.

The System Design Description document provides further details on the Turbine Island Control and Protection System architecture [31].

## 7.7.5 Cooling Water Island Control and Protection System

The primary function of the Cooling Water Island (CWI) Control and Protection System is to automate, control and protect all the CWI fluid and mechanical process systems, except Essential Services (Cooling) Water System (ESWS), within the RR SMR power station.

CWI Control and Automation systems shall be provided for all operating modes of the power station and shall:

- CWI process is always monitored
- automatically control the CWI process within its operational envelope at all times
- provide CWI operational information and data to operators and management systems
- provide maintenance facilities and fault information
- provide alarms and corrective actions during process envelope excursions, ESWS
- provide a means of operator interaction and intervention in the CWI process

Protection systems shall be provided for all operating modes of the power station and shall:

- CWI processes can be safely terminated or corrected
- provide corrective actions during process envelope excursions
- provide automated protection functions to the CWI processes



- protect the nuclear processes in the manner prescribed within the Safety Case
- protect plant, personnel and the environment in the manner prescribed within the Safety Case.

The System Design Description document provides further details on the CWI Control and Protection System design [32].

## 7.7.6 Water Supply Control and Protection System

The primary function of Water Supply Control and Protection System is to control and protect the Water Supply System that receives plant make up water from city mains water network (potable quality water) and supplies water to the following systems/users across the power plant:

- Demineralisation Plant - Treatment and use in Reactor Island and Turbine Island
- Essential Services Water System - make up to ESWS cooling tower
- Main Cooling Water System - Seal flushing on pumps
- Fire Extinguishing System
- Potable Water System
- Cleaning systems
- Water requirements for commissioning of SMR power plant.

## 7.7.7 Demineralisation Treatment Control and Protection System

The primary function of Demineralisation Treatment Control and Protection System is to control and protect the Demineralisation Plant system that produces demineralised water from potable water utilising reverse osmosis and electro deionisation processes.

## 7.7.8 Auxiliary Steam Generating System Control and Protection System

The primary function of Auxiliary Steam Generating System Control and Protection System is to control and protect the Auxiliary steam generating plant that generates low pressure saturated steam and supplies steam to turbine gland seals, main feedwater deaeration requirements and main feedwater heating requirements during plant start up, shutdown and hot standby periods.

## 7.7.9 Security Management Systems

The primary function of the Security Management Systems is to deter, detect and delay an intruder with unauthorised access onto site, provide nuclear security and protect the Power Stations assets. The baseline architecture for the Security system consists of CCTV, access control and intruder detection which interfaces with a central security control system.



The Security Management Systems will have an overarching central security control system which will be split into three sub systems, which are:

- CCTV
- Access Control System
- Intruder Detection System.

### **7.7.10 Building System Control**

The primary function of the system is to monitor and provide supervisory control and coordination of the Building Automation provided by the various specialised systems such as:

- Process Monitoring System
- HVAC Control Equipment (non-nuclear)
- Access control, Surveillance and Intruder Alarm Systems
- General Building Monitoring and Management.

### **7.7.11 Communication and Information Systems**

The primary function of the Communication and Information Systems is to provide Information Technology (IT) communication and information to all RR SMR processes, management and building systems, except for Operational Technology (OT) process systems, within the RR SMR power station.

The Communication and Information Systems comprise of the following subsystems:

- Communication System: It will provide all site-wide voice communications in both normal and accident conditions.
- Information System: It will provide a site loudspeaker/ public address system to provide the ability to broadcast plant warnings and instructions in both normal and accident conditions.
- Information Technology Systems: It will provide the transportation and network communication facilities for the IT data, for the LAN and WAN architecture, Management Information Systems (MIS), Corporate Enterprise Systems, Intranet, and Internet of the SMR nuclear power plant.

### **7.7.12 Instrumentation**

The Instrumentation is primarily made up of sensors for measuring pressure (gauge or differential), temperature, level, flow, radiation, position (e.g., Valve Position or Control Rod Position), and pump speed etc. Where possible, instrumentation will be standardised across the RR SMR plant and shall be selected from a Standard Equipment list. Due to the nature of the environment within some of the Islands, for example, RI, it is envisaged that some of the instrumentation will not be standard.

All instrumentation used in nuclear safety applications shall be designed to applicable codes and standards, and will need to be justified as suitable for the relevant applications. Instrumentation



which do not have nuclear safety applications can generally be chosen from commercial off the shelf equipment and shall satisfy less stringent codes and standards.



## 7.8 C&I Essential Support Systems

---

The C&I systems rely upon and provide control and monitoring of Reactor Island essential support services for C&I.

Essential support services equipment failures can result in the unavailability of C&I systems that provide duty functions, preventative, protective or mitigating measures. Where practicable, the C&I systems design includes features to cater for such failures (e.g., safe modes of failure, detection and alarms). The support function is categorised the same as the measure it supports, and the support system is classified the same as the C&I system it supports.

The essential support services are being developed at RD7/DRP1, and include:

- HVAC. E3S Case Version 2, Tier 1, Chapter 9A: Auxiliary systems [33] describes the HVAC design at RD7/DRP1 maturity, including the provision of providing cooling to safety classified C&I.
- Electrical power distribution. ES3 Case Tier 1 Chapter 8: Electrical Power [10] describes the electrical power systems design at RD7/DRP1 maturity, including how independence and diversity of power supply is achieved for C&I.



## 7.9 Human Machine Interface

---

### 7.9.1 Main Control Room

The MCR is located within Reactor Island inside the Hazard Shield. Permanently staffed, the MCR is the primary location for the control and management of activities related to the reactor and power generation. It will be designed in accordance with Human Factors requirements, as described in E3S Case Version 2, Tier 1, Chapter 18: Human Factors Engineering, Reference [34].

The MCR is provided with information and control facilities from/to the entire C&I system architecture and supports control and monitoring functions for all operational states. The main operator interfaces for plant control are computerised, comprising both individual operator workstations and large wall-mounted displays that provide a plant overview and support co-ordinated operations. The control locations incorporate adequate physical separation to maintain independence of C&I safety systems and physical separation between redundant divisions of protection systems.

Safety critical RPS [JRA] displays will be digital, while manual controls are assumed to be hardwired. A minimal hardwired HMI provides a class 1 interface to the DPS [JQA] sufficient for actuation and monitoring of all the DPS category A functions.

The AMS [JRQ] indicates the values of variables needed by plant operators in accident conditions, to enable them:

- To take pre-planned manual actions to bring the plant to a safe state
- To determine whether the FSFs are being fulfilled
- To determine the potential for a breach or the presence of an actual breach of the barriers preventing release of fission products (e.g., the fuel cladding, the reactor coolant pressure boundary, and the containment)
- To determine the status and performance of plant systems necessary to mitigate consequences in design basis accidents and design extension conditions, and bring the plant to a safe state
- To determine the need to initiate action to protect the public from a release of radioactive material
- To implement the Severe Accident Management Safety Guidelines at the plant

The MCR is fitted with sufficient systems and equipment to deliver safe plant operation in all modes. The MCR includes provision of an overview information system, together with individual workstations to facilitate specific function delivery.

The control room design provides a modern ergonomic control environment for plant operators.



## 7.9.2 Supplementary Control Room

A SCR is provided to allow shutdown and then continued monitoring and control of systems and equipment in the event of MCR evacuation.

The SCR is physically and electrically separated from the MCR, such that the impact on SCR availability from an event affecting the MCR is minimised. The control locations incorporate adequate physical separation to maintain independence of C&I safety systems and physical separation between redundant divisions of protection systems. The RPS [JRA] and DPS [JQA] each have dedicated displays and operator controls, independent of each other and all other systems.

The operational control and management of the 'Transfer of Control' process, to hand plant control priority over from the Main Control Room to the Supplementary Control Room, is expected to be initiated from a location outside of the MCR.

The Supplementary Control Room is expected to be located within Reactor Island but outside of the Hazard Shield. The SCR will be used to control and monitor aspects of the reactor and associated systems in the event that the MCR has to be evacuated.

## 7.9.3 Emergency Response Centre

An Emergency Response Centre is provided on-site, located within Reactor Island but outside of the Hazard Shield. The Emergency Response Centre is used to co-ordinate activities in response to emergencies such as fires or radiation emergencies.

It will include facilities such as CCTV, IT, communication equipment and PPE such as dosimeters. This facility is not permanently staffed. The Emergency Response Centre will include the ability to monitor plant status (via normal operator interfaces) but no control capabilities will be provided.

The Emergency Response Centre is physically separate from the MCR and the SCR, such that the impact on Emergency Response Centre availability from an event affecting the MCR or SCR is minimised.

## 7.9.4 Technical Support Centre

A Technical Support Centre (TSC) is also located within Reactor Island outside of the Hazard Shield and is staffed by technical engineers who support the Control Room operators during abnormal operations.

The TSC includes facilities such as IT, communications equipment, and display of parameters shown in the Control Room via normal operator interfaces. The next project phase will consider options to combine this with other control centres (e.g., Emergency Response Centre).

## 7.9.5 Off-Site Emergency Response Centre

An Off-Site Emergency Response Centre is provided outside of the RR SMR site boundary. This Off-Site Emergency Response Centre provides the off-site co-ordination to responses which cannot be managed at the RR SMR site e.g., accidents leading to an off-site radiological hazard.



This Emergency Response Centre is assumed to include IT and communications equipment and will display key parameters at the power station. The next phase of the project will consider if this could be shared across multiple sites and could be part of the fleet support capability.

Other Control Centres (e.g., Security Control Centre, Outage Control Centre) will also exist on the power plant, but are not relevant to Reactor Island C&I.

## 7.9.6 Local HMI Systems

HMI systems are provided in the different plant control and monitoring areas with sufficient redundancy and user friendliness to accommodate the constraints from plant operation and maintenance.

The HMI design makes best use of available technologies to facilitate delivery of the role of the operator.

## 7.10 Conclusions

---

### 7.10.1 ALARP, BAT, Secure by Design, Safeguards by Design

The design of all SSCs presented in this chapter are developed in accordance with the systems engineering design process. This includes alignment to RGP and OPEX, design to codes and standards according to the safety classification, and a systematic optioneering process with down-selection of design options based on assessment against relevant criteria that ensure risks are reduced to ALARP, apply BAT, and are secure by design and safeguards by design, as described in E3S Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules for SSCs [8]. This provides confidence that claims can be met when the full suite of arguments and evidence is developed.

The overall demonstration of ALARP, BAT, secure by design and safeguards by design at RD7/DRP1 is presented in E3S Case Version 2, Tier 1, Chapters 24, 27, 32 and 33 respectively.

### 7.10.2 Assumptions & Commitments on Future Dutyholder/Licensee / Permit Holder

None identified in this revision.

### 7.10.3 Conclusions and Forward Look

The generic E3S Case objective is ‘to provide confidence that the RR SMR design will be capable of delivering the E3S fundamental objective as it developed from a concept design into a detailed design’. This confidence is built through development and underpinning of top-level claims across each chapter of the E3S Case, through supporting arguments and evidence. The top-level claim for chapter 7 is ‘Instrumentation and Control systems are conservatively designed and verified to deliver E3S functions through-life, in accordance with the E3S design principles, to reduce risks to ALARP, apply BAT and in line with Secure-by-Design and Safeguards-by-Design’.

The arguments and evidence presented to meet the generic E3S Case objective at Version 2 include the allocation of C&I safety functions to individual C&I systems which are categorised in accordance with the E3S categorisation and classification methodology, with systems assigned both a safety and seismic classification. Safety measures are specified across each level of DiD with the overall C&I architecture then allocating C&I safety functions to different C&I systems based on the safety measure and aligning with DiD levels.

The Reactor Island C&I SSC design at RD7/DRP1 is developed and evaluated in accordance with the E3S design principles through the integrated E3S and engineering processes [8], including design optioneering, to drive risk reduction to ALARP, and to demonstrate BAT, secure by design and safeguards by design. For example, selection of the N+1 redundancy for RPCS, to provide an optimised position with respect to achieving reliability targets. Environment, security, and safeguards aspects are also considered, for example, enforcing one-way communications from the RPS systems performing category A functions to other RPS systems performing category B supports cyber security. Such design considerations provide confidence that environment, security, and safeguards functions can be achieved by the design as functional requirements are derived through ongoing and iterative E3S analyses.



Further arguments and evidence to underpin claims will be developed in line with the E3S Case Route Map [3] and reported in future revisions of the generic E3S Case, which will further build confidence that the RR SMR can deliver its fundamental E3S objective. This broadly includes refinement of safety requirements, as well as identification of environment, security, and safeguards requirements.



## 7.11 References

---

- [1] Rolls-Royce SMR Limited, SMR0004272 Issue 3, "Reactor Island C&I Codes and Standards Selection Report," January 2024.
- [2] Rolls-Royce SMR Limited, SMR0004294 Issue 3, "Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 1: Introduction," May 2024.
- [3] Rolls-Royce SMR Limited, SMR0002155 Issue 3, "E3S Case Route Map," November 2023.
- [4] Rolls-Royce SMR Limited, SMR0003977 Issue 3, "Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 15: Safety Analysis," May 2024.
- [5] Rolls-Royce SMR Limited, SMR0004444 Issue 3, "Rolls-Royce SMR Fault Schedule (Version 7)," January 2024.
- [6] Rolls-Royce SMR Limited, SMR0007556 Issue 1, "SMR – System Design Description – Reactor Island Control and Protection Systems [JY]," October 2023.
- [7] Rolls-Royce SMR Limited, SMR0000510 Issue 2, "Rolls-Royce SMR C&I Engineering Schedule," June 2023.
- [8] Rolls-Royce SMR Limited, SMR0004589 Issue 3, "Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 3: E3S Objectives and Design Rules," May 2024.
- [9] Rolls-Royce SMR Limited, SMR0003771 Issue 3, "Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 6: Engineered Safety Features," May 2024.
- [10] Rolls-Royce SMR Limited, SMR0004010 Issue 3, "Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 8: Electrical Power," May 2024.
- [11] Rolls-Royce SMR Limited, SMR0004619 Issue 1, "SMR: Controls & Instrumentation - Design for EMIT Strategy," August 2023.
- [12] Rolls-Royce SMR Limited, SMR0004666 Issue 2, "C&I Safety and Cyber Security Integration Strategy," January 2024.
- [13] British Standard BS EN IEC 61226, "Nuclear Power Plants – Instrumentation and Control Important to Safety- Classification of Instrumentation and Control Functions," September 2009.
- [14] BSI, "BS EN IEC 63147, Criteria for accident monitoring instrumentation for nuclear power generating stations," BSI Group, 2017.
- [15] BSI, "Nuclear power plants – Instrumentation, control and electrical power systems – Guidance for the application of IEC 63147:2017/IEEE Std 497™-2016," BSI Group, 2017.
- [16] Rolls-Royce SMR Limited, SMR0006518 Issue 1, "Rolls-Royce SMR Environment, Safety, Security and Safeguards Categorisation and Classification Method," July 2023.
- [17] Rolls-Royce SMR Limited, SMR0001391 Issue 2, "Rolls-Royce Small Modular Reactor Seismic Performance," October 2022.
- [18] Rolls-Royce SMR Limited, SMR0007783 Issue 1, "SMR System Design Description – Reactor Plant Control System [JSA]," November 2023.
- [19] Rolls-Royce SMR Limited, SMR0005213 Issue 1, RR SMR Power Station Operating Philosophy, July 2023.
- [20] Rolls-Royce SMR Limited, SMR0004619 Issue 1, "SMR: Controls & Instrumentation - Design for EMIT Strategy," September 2023.



- [21] Rolls-Royce SMR Limited, SMR0008081 Issue 1, "Approach to Verification of C&I Systems," October 2023.
- [22] Rolls-Royce SMR Limited, SMR0008369 Issue 1, "Approach to Integration and Validation of C&I Systems," November 2023.
- [23] Rolls-Royce SMR Limited, SMR0007347 Issue 1, "System Design Description for the Reactor Protection System [JRA]," October 2023.
- [24] Rolls-Royce SMR Limited, SMR0007690 Issue 1, "System Design Description for the Diverse Protection System [JQA]," October 2023.
- [25] Rolls-Royce SMR Limited, SMR0008137 Issue 1, "DPS [JQA] Architecture," October 2023.
- [26] IEC, "BS EN IEC 61226:2021 Nuclear power plants - Instrumentation, control and electrical power systems important to safety - Categorization of functions and classification of systems," BSI, 2021.
- [27] Rolls-Royce SMR Limited, SMR0005258 Issue 1, "Severe Accident Management Strategy," May 2023.
- [28] Rolls-Royce SMR Limited, SMR0008638 Issue 1, "SMR System Design Description - Accident Management System [JRQ]," January 2024.
- [29] Rolls-Royce SMR Limited, SMR0007782 Issue 1, "SMR System Design Description - Reactor Plant Monitoring System [JSS]," November 2023.
- [30] Rolls-Royce SMR Limited, SMR0006126 Issue 2, "SMR System Design Description - Feedwater, Steam & Condensate Control & Protection System [LY]," August 2023.
- [31] Rolls-Royce SMR Limited, SMR0005933 Issue 2, "SMR System Design Description - Turbine Island Control & Protection System [MY]," August 2023.
- [32] Rolls-Royce SMR Limited, SMR0005562 Issue 1, "Cooling Water Island Control & Protection [PY] System Design Description," August 2023.
- [33] Rolls-Royce SMR Limited, SMR0003863 Issue 3, "Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 9A: Auxiliary Systems," May 2024.
- [34] Rolls-Royce SMR Limited, SMR0004520 Issue 3, "Environment, Safety, Security and Safeguards Case Version 2, Tier 1, Chapter 18: Human Factors Engineering," May 2024.



## 7.12 Appendix A: Claims, Arguments, Evidence

Table 7.12-1 provides a mapping of the claims to the corresponding sections of the chapter that summarise the arguments and/or evidence. The full decomposition of claims and link to underpinning Tier 2 and Tier 3 information containing the detailed arguments and evidence is presented in the E3S Case Route Map [3]. The route map includes the trajectory of Tier 2 and Tier 3 information as the generic E3S Case develops, which will be incorporated into Tier 1 chapters as it becomes available and in line with generic E3S Case issues described in [2].

**Table 7.12-1: Mapping of Claims to Chapter Sections**

Claim	Section of Chapter 7 containing arguments / evidence summary
Overall I&C systems Non-Functional System Requirements are complete	7.1.2.2
Overall I&C systems Non-Functional System Requirements are correctly assigned	7.1.2.2
Overall I&C systems codes and standards are correctly assigned	7.0.3
The requirements allocated to I&C systems from Plant Systems have complete coverage	7.1.2
The allocation of Safety Requirements for the I&C systems are complete	7.1.1
The allocation of Environmental Functional Requirements for the I&C systems are complete	None at this revision
The allocation of Security Functional Requirements for the I&C systems are complete	None at this revision
The allocation of Safeguards Functional Requirements for the I&C systems are complete	None at this revision
The I&C systems are classified correctly	7.1.3
The Overall I&C systems achieves its E3S functional requirements	Not covered in this revision
The Overall I&C systems design achieves its E3S non-functional system requirements	Not covered in this revision
The layout design facilitates the Overall I&C systems achieving its E3S requirements	7.1.4
Overall I&C systems design definitions are verified to meet their requirements	Not covered in this revision
The implemented Overall I&C systems are validated to meet their E3S functions	Not covered in this revision



Claim	Section of Chapter 7 containing arguments / evidence summary
Verification of the Overall I&C systems is preserved through its operational life	Not covered in this revision
Class 1 systems <i>Claims structures as for the overall I&amp;C</i>	7.3, 7.4
Class 2 systems <i>Claims structures as for the overall I&amp;C</i>	7.3
Class 3 systems <i>Claims structures as for the overall I&amp;C</i>	7.2, 0



## 7.13 Glossary of Terms and Abbreviations

---

ADS	Automatic Depressurisation System
ALARP	As Low As Reasonably Practicable
AMS	Accident Management System
BS	British Standard
C&I	Control & Instrumentation
CAE	Claims, Arguments, Evidence
CCF	Common Cause Failure
CCS	Component Cooling System
CCTV	Closed-Circuit Television
CoFT	Control of Fuel Temperature
CoR	Control of Reactivity
CoRE	Control of Radiation Exposure
CoRM	Confinement of Radioactive Material
COTS	Commercial off the Shelf
CRCS	Control Rod Control System
CSCS	Cold Shutdown Cooling System
CVCS	Chemical and Volume Control System
CWI	Cooling Water Island
DBA	Design Basis Accident
DBC	Design Basis Condition
DEC	Design Extension Condition
DHR	Decay Heat Removal
DiD	Defence-in-Depth
DOORS	Dynamic Object-Oriented Requirements System
DPCS	Data Processing and Control System
DPS	Diverse Protection System
DRP	Design Reference Point
E3S	Environment, Safety, Security & Safeguards
ECC	Emergency Core Cooling
EMC	Electro-Magnetic Compatibility
EMIT	Examination, Maintenance, Inspection & Testing



EOP	Emergency Operating Procedure
ESWS	Essential Service Water System
FSF	Fundamental Safety Function
GDA	Generic Design Assessment
GER	Generic Environment Report
GSR	Generic Security Report
HLSF	High Level Safety Function
HMI	Human Machine Interface
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
ICBMs	Independent Confidence Building Measures
IEC	International Electrotechnical Commission
IT	Information Technology
LOCA	Loss of Coolant Accidents
LTOP	Low Temperature Over Pressure
MCR	Main Control Room
MKoP	Modular Kit of Parts
N	No or Number
N/A	Not Applicable
NFMS	Neutron Flux Monitoring System
OPEX	Operating Experience
PAMS	Post-Accident Management System
PCD	Preliminary Concept Definition
PCSR	PreConstruction Safety Report
PFD	Probability of Failure on Demand
PIE	Postulated Initiating Event
PLS	Priority Logic Unit
PLS	Priority Logic System
PPE	Personal Protective Equipment
PE	Production Excellence
PSA	Probabilistic Safety Assessment



PWR	Pressurised Water Reactor
RCS	Reactor Control System
RCP	Reactor Coolant Pumps
RD	Reference Design
RGP	Relevant Good Practice
RLPPS	Reactor Limitation and Preventive Protection System
RPCMS	Reactor Plant Control and Monitoring System
RPCS	Reactor Plant Control System
RPS	Reactor Protection System
RR SMR	Rolls-Royce Small Modular Reactor
SAMG	Severe Accident Management Guidelines
SAMS	Severe Accident Management System
SA	Severe Accident
SCR	Supplementary Control Room
SFC	Single Failure Criterion
SG	Steam Generator
SSC	Structure, System and Component
TBD	To Be Determined
TSC	Technical Support Centre
UK	United Kingdom
V&V	Verification and Validation
Y	Yes