Partner Document Number	Partner Document Issue /Revision	Retention category:
n/a	n/a	A

Title

E3S Case Chapter 7: Instrumentation & Control

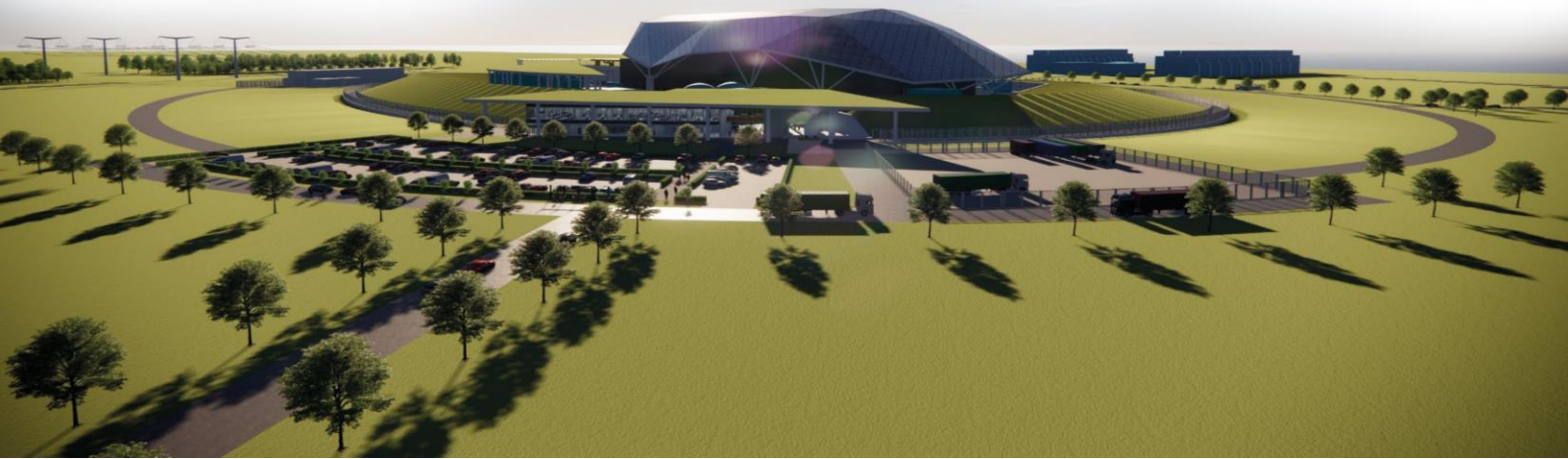
Executive Summary

This chapter of the Environment, Safety, Security, and Safeguards (E3S) Case presents the Control & Instrumentation (C&I) of the Rolls-Royce Small Modular Reactor (RR SMR). The chapter outlines the arguments and preliminary evidence available at the Preliminary Concept Definition (PCD) design stage to underpin the high-level Claim that the RR SMR C&I is designed and substantiated to achieve functional and non-functional safety requirements through the lifecycle and reduce risks to As Low As Reasonably Practicable (ALARP).

The overall C&I architecture is presented based on non-functional system requirements derived from United Kingdom (UK) and international Relevant Good Practice (RGP) and Operating Experience (OPEX). The architecture is presented for 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].

The full suite of evidence to underpin the claim is still in development that will be reported in future revisions of the E3S Case, including further requirements definition and traceability to the Fault Schedule, detailed design definition for each system presented (and additional C&I systems such as fuel route or radioactive waste management), the design of essential support systems and Human Machine Interfaces (HMIs), and ultimately substantiation of requirements.

©2023 Rolls-Royce SMR Ltd all rights reserved – copying or distribution without permission is not permitted



Contents

Tables

Figures

7.0 Introduction

7.0.1 Introduction to Chapter

Chapter 7 of the Rolls-Royce Small Modular Reactor (RR SMR) Environment, Safety, Security and Safeguards (E3S) Case forms part of the Pre-Construction Safety Report (PCSR) and is a supporting reference to the Generic Environment Report (GER) and Generic Security Report (GSR), as defined in E3S Case Chapter 1: Introduction, Reference [1].

Chapter 7 presents the overarching summary and entry point to the design information for the Control & Instrumentation (C&I) systems of the Rolls-Royce Small Modular Reactor (RR SMR), as defined at Reference Design (RD) 5 level of design maturity. 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

The scope of this report covers Reactor Island Control & Protection System [JY]. Within that, the systems in the scope of this revision of the PCSR include the Reactor Protection System (RPS) [JRA], the Diverse Protection System (DPS) [JQA], the Accident Management System (AMS) [JRQ], and the Reactor Plant Control System (RPCS) [JSA]. It also covers the C&I aspects of the RR SMR Human Machine Interfaces (HMIs).

The report includes the overall architecture for the Reactor Island Control & 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).

Environment and Security Functional Requirements for Structures, Systems, and Components (SSCs) will be reported in the GER and the GSR respectively and are not included in the scope of the PCSR.

Design/Programme Maturity

RR SMR design information presented in this revision of the PCSR is largely based on the design definition at the end of Preliminary Concept Definition (PCD), which is an interim design stage representing RD5 level of design maturity. The SSCs presented in this revision of the report are at a maturity commensurate with this design maturity, broadly that requirement specifications are identified and understood, the design scope is defined and bounded, preferred concepts are selected and are likely to deliver requirements, or a plan for down-selection of multiple options is in place.

At PCD, the design of further C&I systems is still being developed, including those for the fuel route, reactor monitoring, radioactive waste management, radiation monitoring, areas of the plant outside Reactor Island [R01], and further design development of essential support systems and HMIs. These will be presented in a future revision of the E3S Case as evidence is developed (see Section 7.0.3).

7.0.3 Claims, Arguments, Evidence Route Map

The Chapter level Claim for E3S Case Chapter 7: Instrumentation & Control is:

Claim 7: The RR SMR Control & Instrumentation is designed and substantiated to achieve functional and non-functional safety requirements through the lifecycle, and reduce risks to As Low As Reasonably Practicable

A decomposition of this Claim into Sub-Claims, Arguments, and link to the relevant Tier 2 Evidence is provided in Appendix A. For each lowest level Sub-Claim, the sections of this report providing the Evidence summary are also identified.

The complete suite of evidence to underpin the Claims in the E3S Case will be generated through the RR SMR design and E3S Case programme and documented in the Claims, Arguments, Evidence (CAE) Route Map, Reference [2], described further in E3S Case Chapter 1: Introduction, Reference [1].

7.0.4 Applicable Regulations, Codes & Standards

The C&I systems summarised in this report are designed to the codes and standards outlined in Table 7.0-1. The British Standards (BS EN) reflect the International Electrotechnical Commission (IEC) standards framework, and these standards are applied to the RR SMR C&I systems according to their classification, and as applicable to the technology used to implement the system.

Table 7.0-1: Standards Applicable to C&I Systems

C&I System	Category C	Category B	Category A
Lifecycle	IEC 61513	IEC 61513	IEC 61513
Hardware	IEC 60987	IEC 60987	IEC 60987
Programmable	IEC 62138	IEC 62138	IEC 60880 (or IEC 62566)
Communications	-	-	IEC 61500
Common Cause Failure (CCF)	-	IEC 62340	IEC 62340
Testing	IEC 60671	IEC 60671	IEC 60671
Separation	IEC 60709	IEC 60709	IEC 60709
Qualification	IEC 60780	IEC 60780	IEC 60780
Seismic	IEC 60980[1]	IEC 60980	IEC 60980
Electro-Magnetic Compatibility (EMC)	IEC 61000	IEC 61000	IEC 61000

C&I System	Category C	Category B	Category A
Control Rooms	IEC 60964 and IEC 60965	IEC 60964 and IEC 60965	IEC 60964 and IEC 60965

[1]Only where Category C functions are expected to be available following a seismic event

7.1 Overall Control & Instrumentation

7.1.1 Overall Architecture, Functions & Functional Allocation

The deterministic safety analysis presented in E3S Case Chapter 15: Safety Analysis, Reference [3], provides a systematic evaluation of the credible Postulated Initiating Events (PIEs). High Level Safety Functions (HLSFs) are identified in the Fault Schedule and assigned to each PIE to deliver the three Fundamental Safety Functions (FSFs): Control of Reactivity (CoR), Control of Fuel Temperature (CoFT) and Confinement of Radioactive Material (CoRM).

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 safety functions to three different 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.

At PCD, the functional allocation for Reactor Island C&I systems is illustrated in Figure 7.1-1. The 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. It is noted that accident management, fuel route and waste management functions are not yet sufficiently developed and therefore have not been considered at this stage.

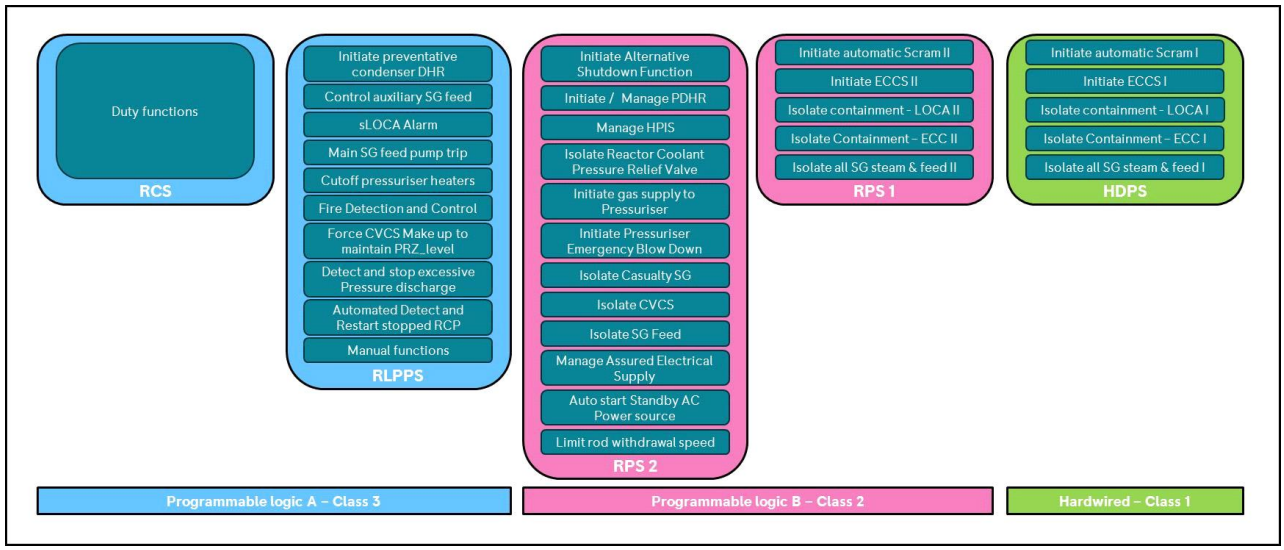


Figure 7.1-1: Reactor Island C&I Architecture (1)

The Reactor Island C&I architecture schematic presented in Figure 7.1-2 shows only the external interfaces and the internal interfaces between the main C&I systems. This both establishes the scope boundary of the Reactor Island [R01] C&I and identifies the interfaces that require definition from both safety and security points of view.

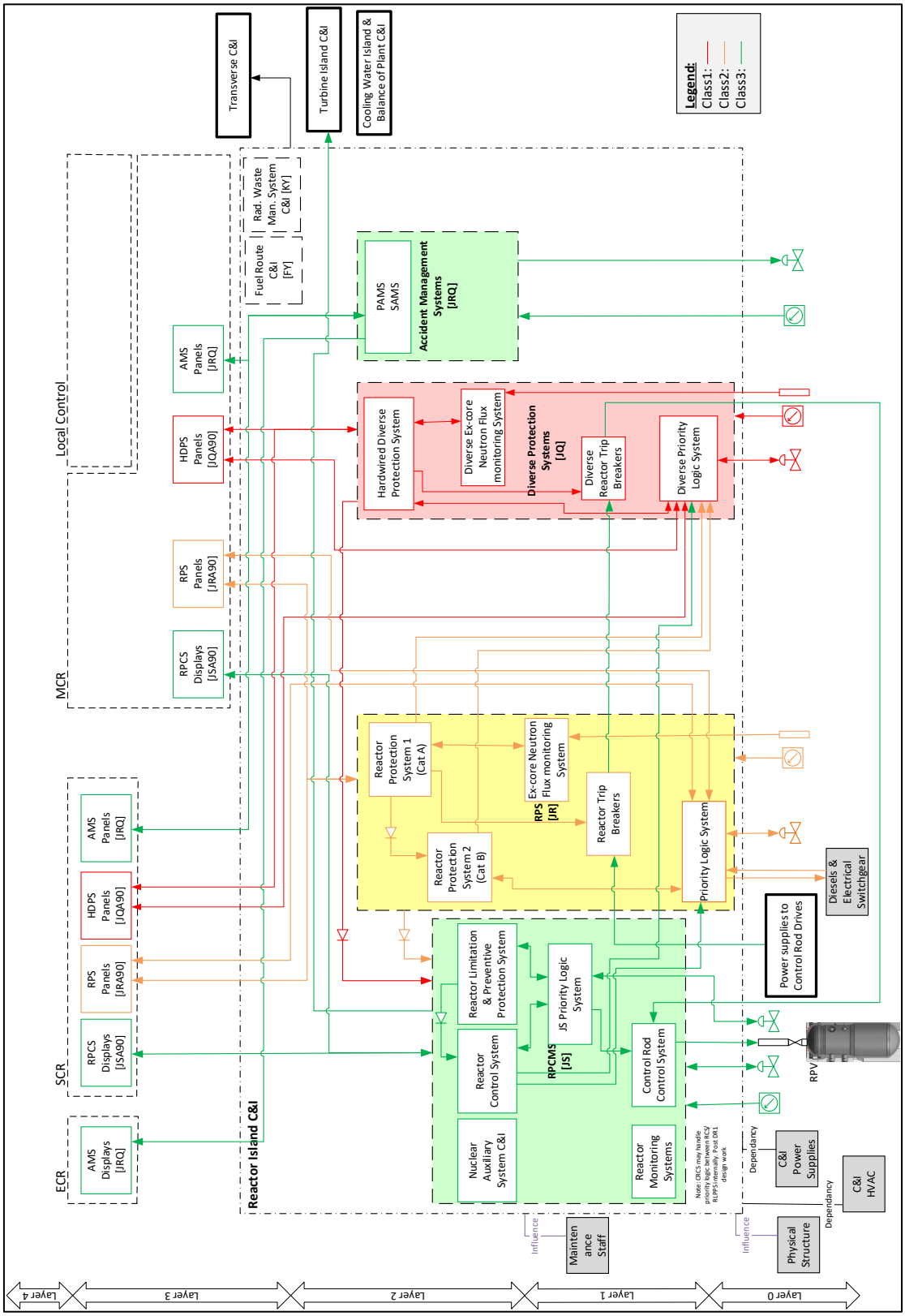


Figure 7.1-2: Reactor Island C&I Architecture (2)

A detailed description of the Reactor Island Control & Protection System [JY] is presented in the System Outline Description in Reference [4], and summarised in this report.

7.1.2 Design Basis

Functional Requirements

The allocation of safety functions to C&I systems and associated Safety Functional Requirements are listed in the Reactor Island Control & Protection System [JY] modules of the requirements management system DOORS (Dynamic Object-Oriented Requirements System). The C&I Engineering Schedule, Reference [5] supports that allocation by arranging C&I functions into appropriate DiD groups.

Non-Functional System 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 C&I DOORS requirements module.

Defence-in-Depth

The five levels of DiD for the RR SMR are described in E3S Case Chapter 3: E3S Objectives & Design Rules, Reference [6], 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:

1. 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 Chapter 6: Engineered Safety Features, Reference [7]), comprising the RPS 1 [JRA10] and RPS 2 [JRA20]

2. The DPS [JQA], a hardwired (i.e., not programmed electronics) system providing the primary means of reactor protection

3. The RPCS [JSA], a second programmed electronics system that is diverse from the RPS [JRA] and provides reactor control functions, comprising of the Reactor Control System (RCS) [JSA10] and the Reactor Limitation & Preventive Protection System (RLPPS) [JSA20], The RPCS [JSA] is part of the overall Reactor Plant Control & Monitoring System (RPCMS) [JS]

4. The AMS [JRQ], supporting all nuclear accident management systems, comprising the Post-Accident Management System (PAMS) [JRQ10] and Severe Accident Management System (SAMS) [JRQ20]. In the event of a serious incident, an Emergency Control Centre (ECC) is also available to enable management of an emergency response, including coordination of on-site and off-site emergency response teams

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

Table 7.1-1: Defence-in-Depth levels of Systems

C&I System	RPCS (RCS)	RPCS (RLPPS)	RPS	DPS	AMS
DiD level	1	2	3	3	3 & 4

Qualification

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. 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	Yes	Yes	Yes	Yes
Seismic*	-	Yes	Yes	Yes
EMC	Yes	Yes	Yes	Yes
Lifecycle (application)	Yes	Yes	Yes	Yes
Lifecycle (platform)	Yes	Yes	Yes	Yes
Lifecycle (smart devices)	Yes	N/A	N/A	N/A

Note: * Seismic qualification requirements are a judgment at present but may change dependent on the equipment locations determined as the design progresses

Failure Behaviour

The concept of fail-safe design is incorporated, as appropriate, into the design of systems and components important to safety. 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.

Redundancy & Independence

All Reactor Island [R01] Class 1 and Class 2 safety systems have redundant divisions. Class 1 systems are designed for compliance with the single failure criterion with the provision of three redundancies, with the safety function being delivered considering a single failure and an outage for maintenance of a whole train. Loss of a train due to the initiating event is not assumed at PCD, to be confirmed through detailed hazards analysis. The C&I System redundancies at PCD are provided in Table 7.1-3, noting the number of redundancies for the DPS [JQA] is being reviewed and therefore are subject to change as the design progresses (see Section 7.1.6).

Table 7.1-3: C&I System Redundancies

C&I System	RPCS	RPS	DPS	AMS
Redundancy	N+1	N+2	N+2	N+1
Implementation	Various (e.g., median selection, hot standby)	2 out of 3 (2oo3)	2oo3	1oo2

Interference between safety systems or between redundant elements of a system is prevented by physical separation, electrical isolation, functional independence, and independence from the effects of communications errors, as appropriate. The associated design rules and sensor sharing policy are summarised in the System Outline Description, Reference [4].

Common Cause Failure & Diversity

Independence and diversity are applied across the overall C&I architecture to address potential for CCF.

Two diverse systems are incorporated in the C&I architecture to deliver all Category A safety functions at DiD level 3; the RPS [JRA] and the hard-wired DPS [JQA]C&I. The RPS [JRA] and the DPS [JQA] at DiD level 3 are diverse from the RPCS [JSA] at DiD levels 1 and 2.

Diversity of C&I systems will continue to be developed as the design matures.

Several different types of diversity are provided within the design:

1. Design diversity: Use of different design approaches to solve the same problem
2. Signal diversity: Safety action is initiated based upon different plant parameters
3. Equipment diversity: System design and hardware employs different technology
4. Functional diversity: Systems perform different functions to achieve the same safety outcome
5. Development diversity: Use of different organisations, different management teams, different design and development teams, different implementation, and testing teams
6. Logic diversity: Use of different logic description languages, different algorithms, different timings, different sequencing of logical functions

The diversity between C&I Systems are indicated in Table 7.1-4.

Table 7.1-4: Diversity within and between C&I Systems

System A	System B	Design diversity	Signal diversity	Equipment diversity	Functional diversity	Development diversity	Logic diversity
Division X	Division Y	N	N	N	N	N	N

System A	System B	Design diversity	Signal diversity	Equipment diversity	Functional diversity	Development diversity	Logic diversity
DPS	RPS	Y	Y[2]	Y	Y[2]	Y	Y
DPS	RPCMS	Y	Y[1]	Y	Y	Y	Y
DPS	AMS	N	TBC	N	N	N	N
RPS	RPCMS	Y	Y[1]	Y	Y	Y	Y
RPS	AMS	N	TBC	N	N	N	N
RPCMS	AMS	N	Y	N	N	N	N

[1]At the present stage of design, the expectation is that, as a minimum, any sensors used for protection against PIEs will not also be used for control purposes that could cause those same events. Similarly, for any sensors that must be shared between the protection systems (though this will be avoided wherever practicable), each system will have another diverse means of detecting all PIEs that are detected using the shared sensor.
[2]Some exceptions may exist, depending on the fault schedule.

Reliability

The reliability requirements placed on the C&I systems are commensurate with the safety significance of the individual systems, presented in Table 7.1-5.

Table 7.1-5: System Safety Integrity Objectives

C&I System	RPCS	RPS[1]	DPS[1]	AMS
Safety Function	1E-2 Probability of failure per demand (PFD) (TBC)	1E-3 PFD (TBC)	1E-4 PFD	1E-2 PFD

[1]At this stage of design, the safety integrity values reflect that the primary means of controlling reactivity and ensuring adequate primary inventory and heat removal is provided, further work is planned to investigate improved reliability of the RPS from an ALARP perspective

Examination, Maintenance, Inspection & Testing

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

Redundancy is incorporated into the design to facilitate Examination, Maintenance, Inspection & Testing (EMIT), at a frequency determined by the Probabilistic Safety Assessment (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.

Spurious Failure

The RPS [JRA] and DPS [JQA] each have a target frequency of spurious actuation causing a significant transient <=1E-3/year, and of spurious actuation that does not cause a significant transient <=1E-2/year.

Human Machine Interface

The requirements for the HMIs in the control rooms and for the selection of functions, design consideration, and organization of the HMIs and procedures which are used to verify and validate the functional design, are based on IEC 60964 (Main Control Room (MCR)), Reference [8], and IEC 60965 (Supplementary Control Room (SCR)), Reference [9]. These requirements reflect the application of human factors engineering principles as they apply to the HMIs during normal and abnormal plant conditions.

Security

The security degrees and zones are defined by specific risk-based attributes. 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 RPS1 (performing Category A functions, and so also at security degree 1, but in a different zone to the DPS) to RPS2 (performing Category B functions and defined as security degree 2).

The design principles for independence, segregation, and diversity, outlined above, also support achievement of security and cyber security concerns. The design will 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.

A De-Militarized Zone (DMZ) will segregate the main plant control systems, network and resources from external service users (e.g., work orders, tag out, digital twin). Physical access to systems and data connections will be controlled with access indication provided in the MCR.

7.1.3 Classification

The E3S Categorisation & Classification methodology is described in E3S Case Chapter 3: E3S Objectives & Design Rules, Reference [6], with its application to mechanical SSCs presented in various engineering chapters across the E3S case. The approach adopted is consistent with BS IEC 61226, Reference [10]. The Reactor Island C&I Systems are also classified corresponding to the functions they perform:

1. RPCS [JSA] actuates the duty control and monitoring functions for the Reactor Island [R01] systems (neutronic power, primary pressure, Reactor Coolant Pumps, Steam Generator levels etc.) and the Category C preventative functions, provides the rod control system, nuclear auxiliary system C&I and non-safety monitoring functions
2. RPS 2 [JRA20] actuates Category B safety functions and provides the Rod Withdrawal Speed limitation system and is Class 2
3. RPS 1 [JRA10] actuates the back-up Category A safety functions and Scram functions and is Class 2

4. DPS [JQA] actuates the primary Category A safety functions and Scram functions and is Class 1
5. AMS [JRQ] is assumed to be a Class 3 system based on early indication of accident requirements, noting at PCD this is to be confirmed

The classification of the C&I systems is summarised in Table 7.1-6.

Table 7.1-6: C&I System Classifications

C&I System	RPCMS	RPS	DPS	AMS
Class	3	2	1	3

7.1.4 C&I Building Layout

The preliminary Reactor Island C&I location is shown in Figure 7.1-3. The DPS [JQA], RPS [JRA], and AMS [JQR] are all located on an aseismic bearing under the Hazard Shield (shown as a thick black line). The MCR is also located in the building housed under the Hazard Shield.

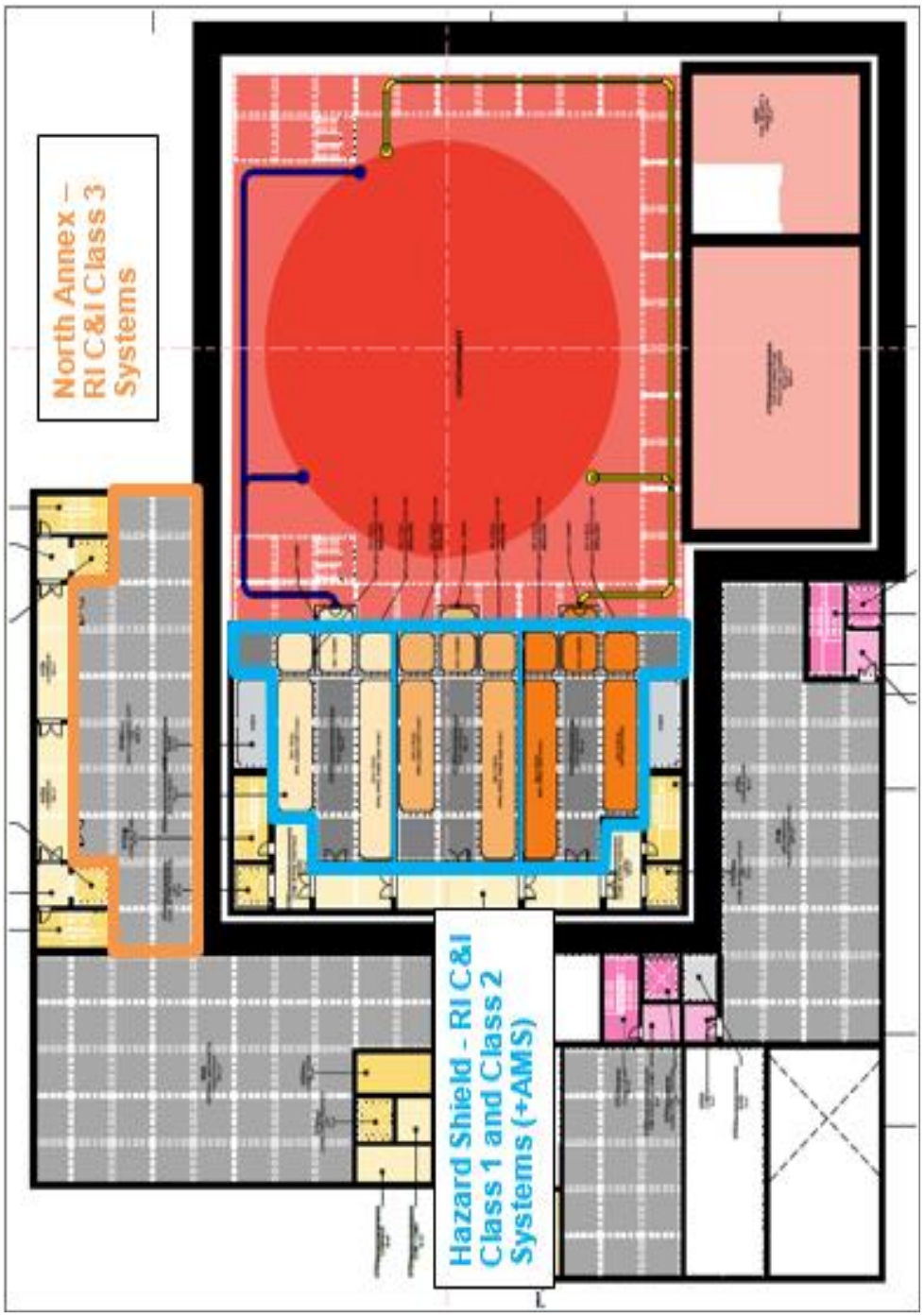


Figure 7.1-3: Preliminary Reactor Island C&I Location

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.

For all actuators which can be controlled by both the DPS [JQA] and RPS [JRA], non-programmable logic units will be used to prioritise between commands. Prioritisation between the RCS [JSA10] and the RLPPS [JSA20] will be done by software. SAMS [JRQ20] actuation should not be shared with other C&I systems and thus does not need prioritisation.

Work to develop the complexities associated with implementing prioritisation logic is ongoing, therefore details will be incorporated into a future revision of the E3S Case as evidence in the CAE Route Map becomes available.

7.1.6 ALARP in Design Development

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 Relevant Good Practice (RGP) & Operating Experience (OPEX), including design rules outlined in Section 7.1.2, 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 PSCR Chapter 3: E3S Objectives & Design Rules, Reference [6]).

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 report.

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.

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, 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 an independence and 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 duty/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 (RPCMS [JS]) has been selected as the PCD 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. An optimised design that shares duty and preventive safety functions on DiD level 1 and 2 respectively, as oppose to independent systems, provides the benefit of a significantly more simplified system with less sensors and cabinets.

Redundancy in Class 1 & 2 Systems

At PCD, the DPS [JQA] (Class 1) and RPS [JRA] (Class 2) each have three redundancies. Optioneering of multiple redundancy options for Class 1 and 2 C&I systems has selected three redundancies as an optimum design position over higher levels of redundancy, on the basis that it offers significant benefits such as a reduced sensor count and system complexity, reduced EMIT burden, and minimises containment and reactor coolant pipework penetrations.

Analysis of three and four-way redundancy options with respect to the probabilistic safety impact has determined that a three-way redundant system can achieve the required reliability targets for each system, whereas increasing the levels of redundancy would provide a slight increase in reliability, however with diminishing safety benefit due to CCFs between the redundancies.

From a deterministic perspective, three redundancies for the DPS [JQA] ensures compliance with the single failure criterion expected for Class 1 systems, to ensure the system can still perform its safety function when demanded in its worst-case configuration, e.g. one train is offline for maintenance and when one train is lost due to single failure. It is recognised that consideration also needs to be made for loss of a train due to a failure or hazard caused by the initiating event itself. As such, the benefits of a 2oo4 system are still being explored at PCD with respect to improving reliability and single failure tolerance of the DPS [JQA]. The outcomes of associated design decisions will be reported in a future revision of the E3S Case as evidence in the CAE Route Map becomes available.

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 (PFD) and spurious actuation.

Priority Logic

For all actuators controllable by the DPS [JQA] or RPS [JRA], non-programmable logic will be used to prioritise between commands and control actuators. Prioritisation between the RCS [JSA10] and the RLPPS [JSA20] will be done via software. 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.

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 PCD 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 Heating, Ventilation and Air Conditioning (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 & Monitoring System

7.2.1 System and Equipment Functions

The RPCMS [JS] comprises the RPCS [JSA] and the Reactor Monitoring System [JSS]. The RPCS [JSA] comprises the following five sub-systems:

1. RCS [JSA10], which provides control and monitoring during normal operation of the primary reactor systems and associated heat exchangers (DiD Level 1 functions)

2. RLPPS [JSA20], which performs functions that detect abnormal operating conditions and failures (DiD level 2 functions) and provides a means, either automatically, or through alarms and operator intervention, to attempt to bring the plant back into normal operation before any limits are breached

3. Control Rod Control System [JSA30], which provides drive power to the control rod drive mechanisms to raise, lower or hold the control rods

4. Nuclear Auxiliary System C&I [JSA40], which is allocated supporting functions related to HVAC systems, power supplies and lighting

5. RPCS Panels & Displays [JSA90], which forms the interface to the operator

The Reactor Monitoring System [JSS] monitors the non-safety critical parameters of the reactor to provide condition monitoring and consists of ten sub-systems.

The RPCS [JSA] contributes to delivery of the following FSFs: CoR, CoFT and CoRM. The full list of allocated functions is provided in the C&I Engineering Schedule, Reference [5].

7.2.2 Design Basis

Functional Requirements

The safety categorised functional requirements for the RPCS [JSA], and associated Non-Functional Performance Requirements, are listed in the DOORS Reactor Island Control & Protection System [JY] Requirements Module.

Non-Functional System Requirements

The non-functional system requirements for the RPCS [JSA] are listed in the Reactor Island Control & Protection System [JY] modules of DOORS, based on the design rules listed in Section 7.1.2.

Categorisation & Classification

The only functions assigned to the RCS [JSA10] that have a safety categorisation is the Control Component Cooling System, which is Safety Category C. The preventative functions assigned to the RLPPS [JSA20] are all Safety Category C. The RCS [JSA10] and RLPPS [JSA20] are therefore both Safety Class 3 with a common platform for simplification and maintenance.

The functions allocated to the Nuclear Auxiliary System C&I [JSA30] are from the HVAC systems, and are Safety Category C. The Nuclear Auxiliary System C&I [JSA30] is therefore Safety Class 3.

No safety categorisation of the RPCS Panel & Displays [JSA90] and the Reactor Monitoring System [JSS] has been undertaken, however it is assumed that there will be no functions assigned that are greater than Safety Category C.

7.2.3 Description

The architecture of the RPCMS [JS] is shown in Figure 7.1-2. For cabinets and communication networks, the design incorporates dual redundancy, likely to function in a 'hot standby' arrangement. For sensors, the design incorporates triple redundancy on each measurement for reliability purposes.

7.2.4 Interfaces

Parameters 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.

7.2.5 System & Equipment Operation

Failure Behaviour

The RPCMS [JS] shall be designed to detect input failures such as loss of communication or out of range signal inputs, system failures such as 'watchdog' timeouts, and output failures such as loss of communication with an actuator.

Voting Logic

At PCD, no voting logic is defined.

7.2.6 EMIT

The Safety Category C functions of the RPCMS [JS] will need to be testable during normal operations. Sensors and actuators shall be tested during outages when the plant is in a mode/state allowing the cycling of valves and removal of sensors for testing.

7.2.7 Preliminary Substantiation

At PCD, an initial, high-level Verification and Validation (V&V) plan for C&I is presented in Reference [11]. It sets out how Verification and Validation for the RPCMS [JS] to meet its safety categorised functional requirements and non-functional system requirements will be approached and identifies some of the key activities.

7.2.8 Installation & Commissioning

An outline installation and commissioning plan for the RPCMS [JS] is still to be developed. The overall strategy for the RR SMR commissioning programme is presented in E3S Case Chapter 14: Plant Construction & Commissioning, Reference [12].

7.2.9 ALARP in Design Development

The design of the RPCMS [JS] has been developed in accordance with the systems engineering design process, which includes alignment to RGP & 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 E3S criteria (as described in PSCR Chapter 3: E3S Objectives & Design Rules, Reference [6]).

Key RPCMS [JS] design decisions made with respect to ensuring overall risks are reduced to ALARP include:

1. Options for single, two, three, and four levels of redundancy have been explored for the RPCMS [JS] cabinets and communication networks to perform duty and preventive safety functions, with the selection of dual redundancy. This is on the basis that two redundancies provide the optimised position with respect to achieving PFD targets and minimising the demand on the protection C&I systems (RPS [JRA] and DPS [JQA]). Compared to higher levels of redundancy, the design offers the benefit of minimising the complexity of operation and EMIT, as well as the overall power demand for the system. Clearly higher levels of redundancy offer increased tolerance to faults, however the safety benefit is expected to be limited due to CCFs and the increased level of complexity increasing the likelihood of spurious failures. This approach aligns to RGP which focuses on increased reliability for Class 1 and 2 systems

2. For sensors, triple redundancy on each measurement has been selected for the PCD design baseline to ensure that for conflicting valid sensor readings the control system is able to determine which reading is suspect, which is simpler to achieve with three sensors than two. As the redundancy is for reliability purposes rather than independence, no separation of signals is needed so all 3 measurements will be made available to each control system redundancy. Further work will be undertaken as the design progresses to confirm this position

Discussion on the development of the overall C&I architecture to reduce risks to ALARP is presented in Section 7.1.6.

7.2.10 Ongoing Design Development

The RR SMR design definition is currently in development as described in Section 7.0.2. Key design opportunities and decisions related to nuclear safety being explored at PCD include:

1. Opportunities to reduce the level of sensor redundancy on a case-by-case basis

All design development risks and opportunities are captured and managed by design teams. Further details of design development will be incorporated into a future revision of the E3S Case as evidence in the CAE Route Map becomes available.

7.3 Reactor Protection System

7.3.1 System and Equipment Functions

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

1. Secondary means of implementing all Safety Category A functions (alongside the DPS [JQA] at DiD level 3, fulfilled by RPS 1 [JRA10]
2. Implementation of DiD level 3 Safety Category B functions, fulfilled by RPS 2 [JRA20]
3. Implementation of DiD level 2 Safety Category B 'Limit rod withdrawal speed' function, also fulfilled by RPS 2 [JRA20]

The RPS [JRA] contributes to delivery of the following FSFs: CoR, CoFT and CoRM. The full list of allocated functions is provided in the C&I Engineering Schedule, Reference [5].

7.3.2 Design Basis

Functional Requirements

The safety categorised functional requirements for the RPS [JRA], and associated Non-Functional Performance Requirements, are listed in the DOORS Reactor Island Control & Protection System [JY] Requirements Module.

Non-Functional System Requirements

The non-functional system requirements for the RPS [JRA] are listed in the Reactor Island Control & Protection System [JY] modules of DOORS, based on the design rules listed in Section 7.1.2.

Categorisation & Classification

The RPS [JRA] provides a secondary means of fulfilling a Safety 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 Chapter 3: E3S Objectives & Design Rules, Reference [6], is classified as Safety Class 2.

7.3.3 Description

Given the independence and diversity between the RPS [JRA] and DPS [JQA], RPS 1 [JRA10] does not need to be diverse from RPS 2 [JRA20]. As such, the design shares a common technology platform, support services, and common signal inputs. It is noted the two systems will be implemented in two physically segregated systems with electrical isolation between them to reduce the probability of CCFs and provide future design flexibility.

Figure 7.3-1 shows the proposed architecture for RPS 2 [JRA20]. RPS 1 [JRA10] will have a similar configuration, with the main difference being that it will interface with the Ex-core Neutron Flux Monitoring System [JRA30] and the Reactor Trip Breakers [JRA40] (which are not shown).

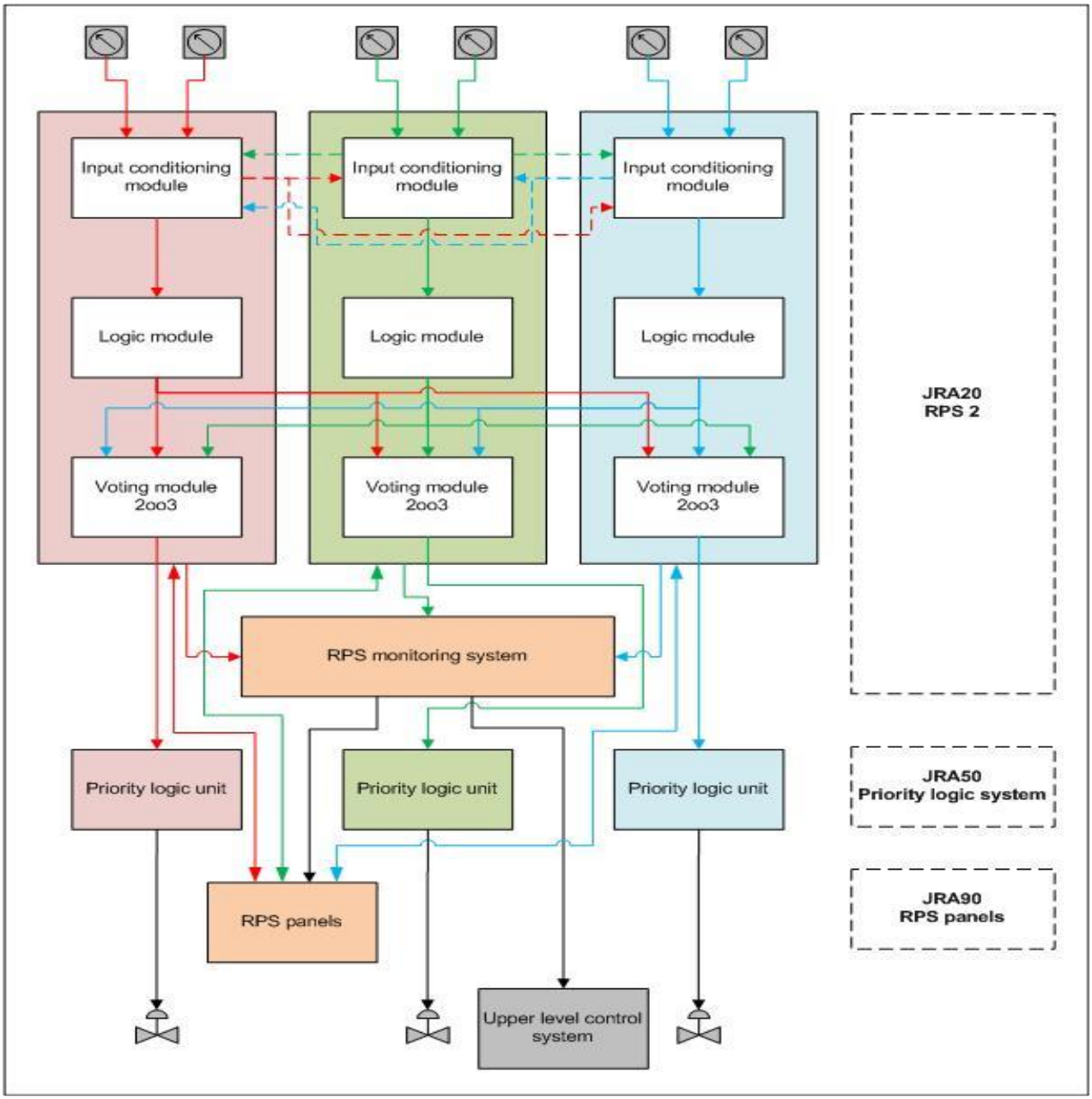


Figure 7.3-1: RPS 2 [JRA20] Architecture

7.3.4 Interfaces

As RPS 1 [JRA10] implements the same Safety Category A functions as the DPS [JQA] it shares many actuators, controlled through a diverse priority logic system (shown in Figure 7.4-1). The RPS [JRA] also has its own set of priority logic system for the actuators driven by the RPS 2 [JRA20] safety functions.

The RPS [JRA] can share data, where the safety analysis allows it, with the lower safety classification RPCMS [JS]. Internally, RPS 1 [JRA10] is permitted to share its input signals with RPS 2 [JRA20], but not the other way around.

There is one ex-core Neutron Flux Monitoring System (NFMS) in the RPS [JRA], which interfaces with RPS 1 [JRA10] that in turn shares its measurement to RPS 2 [JRA20]. The Scram function is only implemented in RPS 1 [JRA10] which interfaces with the RPS Reactor trip breakers, which are connected in series with the control rod drive power supplies and DPS reactor trip breakers.

7.3.5 System & Equipment Operation

Monitoring

Information from the three redundancies needs to be compared to detect sensor drift or failures in the conditioning equipment. Information from all three redundancies needs to be transmitted to the upper-level control system for display and recording. A preliminary architecture for this functionality has been developed, referred to in the System Outline Description, Reference [4].

Failure Behaviour

The RPS [JRA] shall utilise de-energise-to-actuate for Scram [JD01] and energise-to-actuate for other safety measure actuations. The design will be fail-safe.

Voting Logic

During normal operation the three redundancies shall vote in a 2oo3 arrangement to minimise spurious actions. During periodic testing, the redundancy under test/maintenance shall be placed in an un-tripped state and the voting logic shall remain at 2oo3, effectively becoming a 2oo2 system.

7.3.6 EMIT

The sensors of the RPS [JRA] require regular calibration, the frequency and method of this calibration depends on the sensor type.

The RPS [JRA] will also need to be testable during normal operations. Each redundancy will be tested in turn, with its outputs placed in an un-tripped state during the test. Testing time shall be minimised. Overlap testing will be used to test the whole chain from sensor inputs to just before the actuator outputs.

Sensors and actuators shall be tested during outages when the plant is in a mode/state allowing the cycling of valves and removal of sensors for testing.

7.3.7 Preliminary Substantiation

At PCD, an initial, high-level V&V plan for C&I is presented in Reference [11]. It sets out how Verification and Validation for the RPS [JRA] to meet its safety categorised functional requirements and non-functional system requirements will be approached and sets out some of the key activities.

7.3.8 Installation & Commissioning

An outline installation and commissioning plan for the RPS [JRA] is still to be developed. The overall strategy for the RR SMR commissioning programme is presented in E3S Case Chapter 14: Plant Construction & Commissioning, Reference [12].

7.3.9 ALARP in Design Development

The design of the RPS [JRA] has been developed in accordance with the systems engineering design process, which includes alignment to RGP & 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 E3S criteria (as described in PSCR Chapter 3: E3S Objectives & Design Rules, Reference [6]).

Discussion on the development of the overall C&I architecture to reduce risks to ALARP is presented in Section 7.1.6.

7.3.10 Ongoing Design Development

The RR SMR design definition is currently in development as described in Section 7.0.2. Further design developments will be incorporated into a future revision of the E3S Case as evidence in the CAE Route Map becomes available.

7.4 Diverse Protection System

7.4.1 System and Equipment Functions

The primary role of the DPS [JQA] is to implement all automatic Safety Category A functions responding to Design Basis Faults at DiD level 3, contributing to delivery of the following FSFs: CoR, CoFT and CoRM. The full list of allocated functions is provided in the C&I Engineering Schedule, Reference [5].

A secondary role of the DPS [JQA] is to respond to Design Basis Faults that occur simultaneous with a CCF of the RPS [JRA], with diversity and independence between the two systems. The intent is for the DPS [JQA] to react later in the accident progression than the RPS [JRA], such that successful RPS functioning will not require DPS functioning.

7.4.2 Design Basis

Functional Requirements

The safety categorised functional requirements for the DPS [JQA], and associated Non-Functional Performance Requirements, are listed in the DOORS Reactor Island Control & Protection System [JY] Requirements Module.

Non-Functional System Requirements

The non-functional system requirements for the DPS [JQA] are listed in the DOORS Reactor Island Control & Protection System [JY] Requirements Module, based on the design rules listed in Section 7.1.2.

Categorisation & Classification

The DPS [JQA] provides the primary means of fulfilling Safety Category A functions, and in accordance with the E3S Categorisation and Classification methodology outlined in E3S Case Chapter 3: E3S Objectives & Design Rules, Reference [6], it is classified as Safety Class 1.

7.4.3 Description

A simplified architecture for the DPS [JQA] is illustrated in Figure 7.4-1.

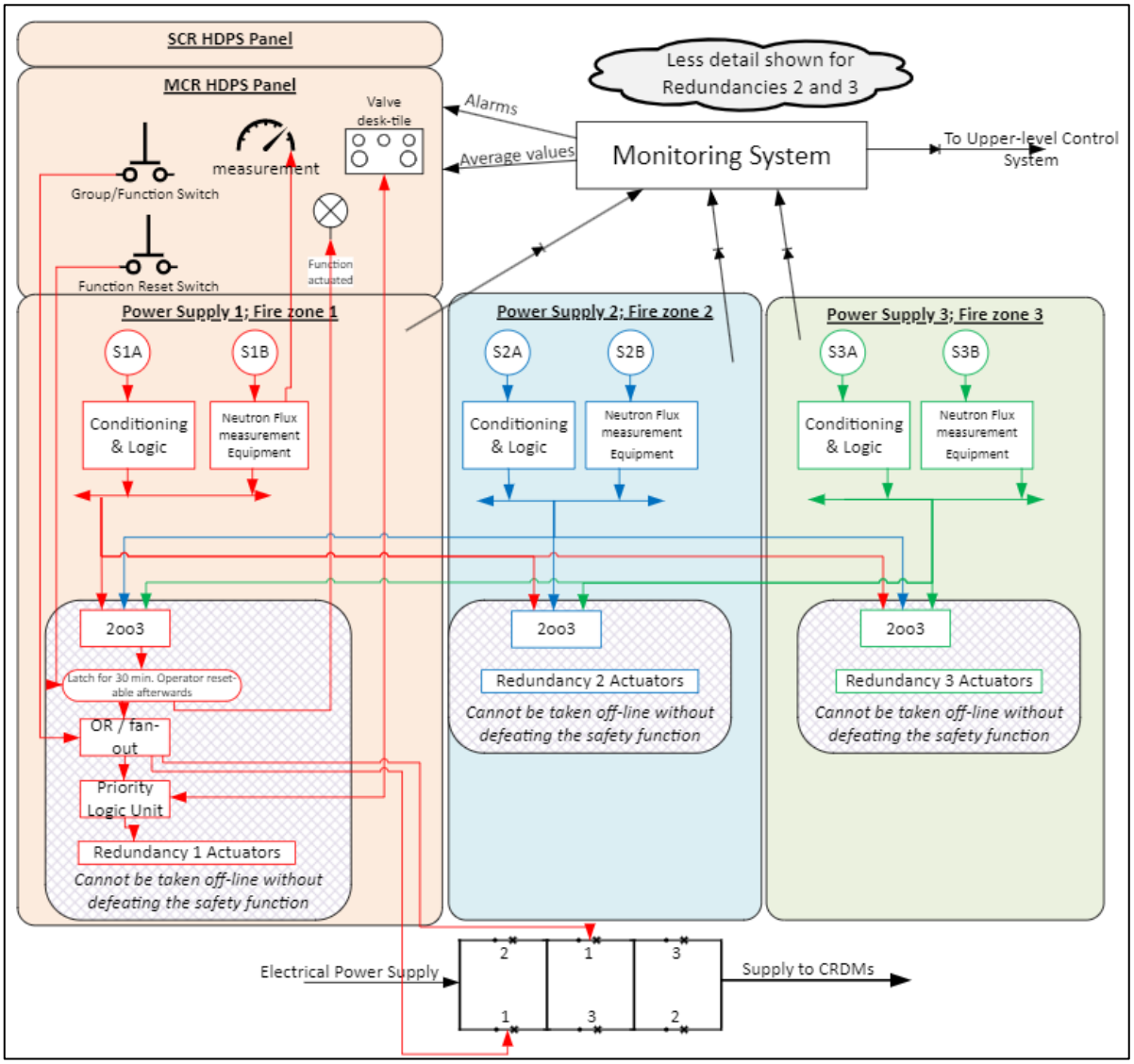


Figure 7.4-1: DPS Architecture

7.4.4 Interfaces

External connections from the DPS [JQA] are included for:

1. One-way communication to the RPCMS [JS] for monitoring and discrepancy checking (TBC)
2. One-way communication to the Accident Management Systems [JRQ]
3. DPS Trip Breakers – Inputs from RPS 1 and 2 (TBC)
4. DPS Priority Logic System – Inputs from RPCMS [JSA] and RPS [JRA]

7.4.5 System & Equipment Operation

Monitoring

Information from the three redundancies needs to be compared to detect sensor drift or failures in the conditioning equipment and transmitted to the upper-level control system for display and recording. The architecture for this functionality is to be determined.

Voting Logic

During normal operation the three redundancies shall vote in a 2oo3 arrangement to minimise spurious actions. During periodic testing, the redundancy under test/maintenance shall be placed in a tripped state and the voting logic shall change to 1oo2.

Failure Behaviour

The DPS [JQA] shall utilise de-energise-to-actuate for Scram [JD01] and energise-to-actuate for other safety measure actuations. The design will be fail-safe where this is technically feasible.

7.4.6 EMIT

The sensors of the DPS [JQA] require regular calibration, particularly ex-core flux, typically done via an adjustable gain which is set at the C&I cabinets according to the calculated thermal power of the plant (during a steady state).

The Safety Category A functions of the DPS [JQA] will need to be tested during normal operations, with a frequency informed by the PSA. MCR HMIs shall also be tested during the regular periodic testing by stimulating displays for operator observation. Sensors and actuators shall be tested during outages when the plant is in a mode/state allowing the cycling of valves and removal of sensors for testing.

7.4.7 Preliminary Substantiation

At PCD, an initial, high-level V&V plan for C&I is presented in Reference [11]. It sets out how Verification and Validation for the DPS [JQA] to meet its safety categorised functional requirements and non-functional system requirements will be approached and identifies some of the key activities.

7.4.8 Installation & Commissioning

An outline installation and commissioning plan for the DPS [JQA] is still to be developed. The overall strategy for the RR SMR commissioning programme is presented in E3S Case Chapter 14: Plant Construction & Commissioning, Reference [12].

7.4.9 ALARP in Design Development

The design of the DPS [JQA] has been developed in accordance with the systems engineering design process, which includes alignment to RGP & 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 E3S criteria (as described in PSCR Chapter 3: E3S Objectives & Design Rules, Reference [6]).

Key DPS [JQA] design decisions made with respect to ensuring overall risks are reduced to ALARP include:

1. A hardwired technology for the DPS [JQA] has been selected to achieve the system requirements, on the basis that a hardwired system follows UK RGP in providing a diverse technology to software-based technologies used in the RPS [JRA]. It also provides a simplified solution with respect to potential failure modes and the verification and validation of the system. A hardwired system is also less vulnerable to cyber security risks than a software-based system

Discussion on the development of the overall C&I architecture to reduce risks to ALARP is presented in Section 7.1.6.

7.4.10 Ongoing Design Development

The RR SMR design definition is currently in development as described in Section 7.0.2. Key design opportunities and decisions related to nuclear safety being explored at PCD include:

1. The benefits of increasing the number of DPS [JQA] redundancies to a 2oo4 configuration with respect to improving reliability and tolerance to single failures

All design development risks and opportunities are captured and managed by design teams. Further details of design development will be incorporated into a future revision of the E3S Case as evidence in the CAE Route Map becomes available.

7.5 Accident Management System

7.5.1 System and Equipment Functions

The role of the AMS [JRQ] is to provide monitoring instrumentation and systems for preventive and mitigative accident management during Design Basis Accidents (DBAs), Design Extension Conditions (DEC), and Severe Accidents (SAs). It comprises the:

1. PAMS [JRQ10], which is part of DiD Level 3 integrates actions and measures needed to prevent significant core damage and terminate the progress of core damage once it has started, usually accomplished by plant operation staff using Emergency Operating Procedures (EOPs) in the MCR or SCR
2. SAMS [JRQ20], which is part of DiD Level 4, maintains the integrity of the containment as long as possible, minimising releases of radioactive material and achieving a long-term stable state when the fuel has started to degrade, usually performed by control room operators using Severe Accident Management Guidelines (SAMGs)

The AMS [JRQ] contributes to delivery of the following FSFs: CoR, CoFT and CoRM. The full list of allocated functions is provided in the C&I Engineering Schedule, Reference [5].

7.5.2 Design Basis

Functional Requirements

The safety categorised functional requirements for the AMS [JRQ], and associated Non-Functional Performance Requirements, are listed in the DOORS Reactor Island Control & Protection System [JY] Requirements Module.

Non-Functional System Requirements

The non-functional system requirements for the AMS [JRQ] are listed in the Reactor Island Control & Protection System [JY] modules of DOORS, based on the design rules listed in Section 7.1.2.

Categorisation & Classification

The AMS [JRQ] delivers Safety Category C functions, and in accordance with the E3S Categorisation and Classification methodology outlined in E3S Case Chapter 3: E3S Objectives & Design Rules, Reference [6], is classified as Safety Class 3. The safety categories and classifications are subject to change as the design matures.

7.5.3 Description

The AMS architecture at PCD is presented in Figure 7.5-1. The PAMS [JRQ10] is intended to be implemented in a programmable technology, while the SAMS [JRQ20] is intended to be implemented in a hardwired technology.

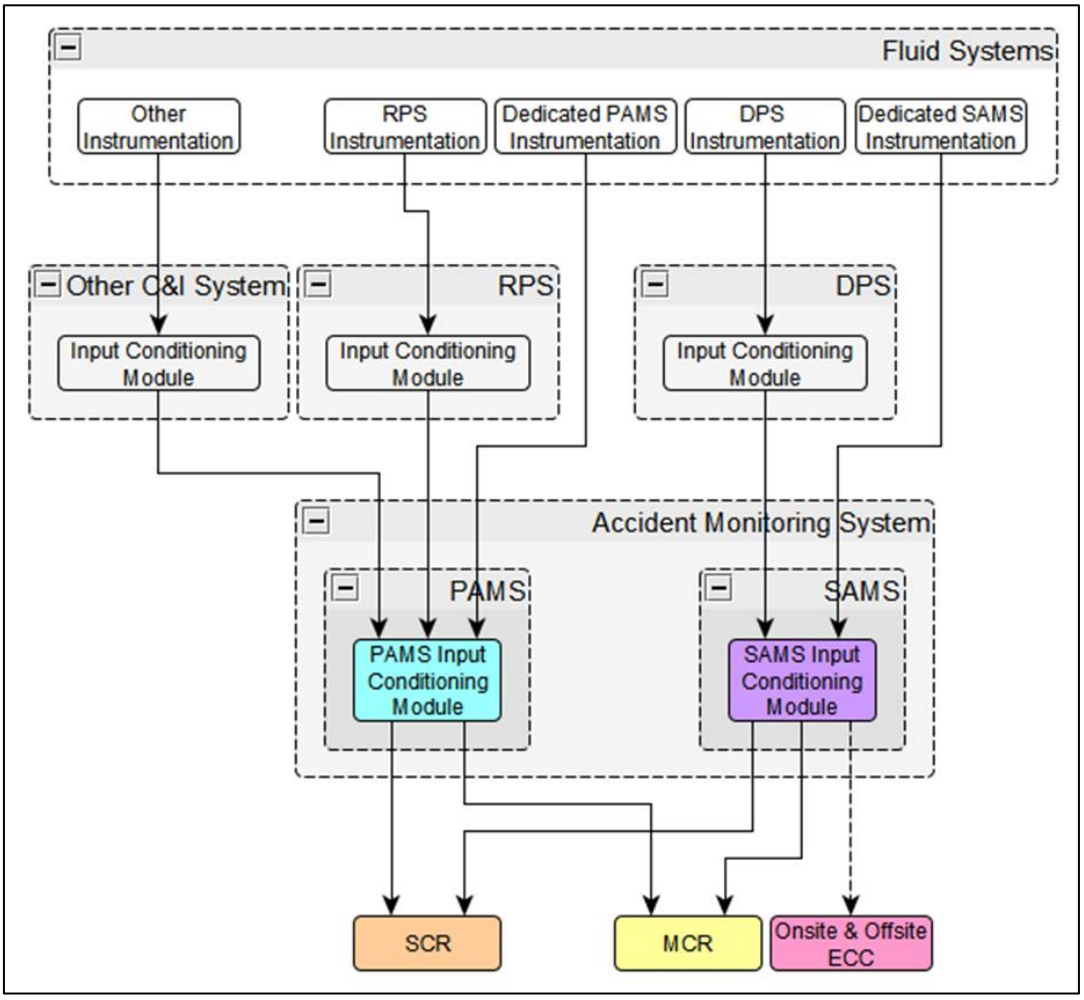


Figure 7.5-1: AMS Architecture

7.5.4 Interfaces

There will be no interconnection between the PAMS [JRQ10] and SAMS [JRQ20]. PAMS [JRQ10] variables are provided via other class 3 or higher classified Reactor Island C&I systems and SAMS [JRQ20] variables via the DPS [JQA]. It is expected that the AMS [JRQ] shall directly monitor some variables on top of what can be provided by the RPS [JRA] and DPS [JQA] functions.

7.5.5 System & Equipment Operation

Monitoring

The monitoring for the AMS [JRQ] is still to be determined.

Failure Behaviour

The AMS [JRQ] shall be designed to fail safely, with automatic detection of out-of-range sensor failures and in-range failures. It is assumed that the SAMS [JRQ20] hardwired HMI display in the control rooms will contain a physical display for each sensor, providing the operators all plausible data and helping identify trends or failures.

Voting Logic

At PCD, no voting logic is required as measured data is displayed directly in the MCR.

7.5.6 EMIT

The sensors of the AMS [JRQ] are expected to require regular calibration. The frequency of this is dependent on the variable type and the specific accident scenario that the sensor is intended to help mitigate.

7.5.7 Preliminary Substantiation

At PCD, an initial, high-level V&V plan for C&I is presented in Reference [11]. It sets out how Verification and Validation for the AMS [JRQ] to meet its safety categorised functional requirements and non-functional system requirements will be approached and identifies some of the key activities.

7.5.8 Installation & Commissioning

An outline installation and commissioning plan for the AMS [JRQ] is still to be developed. The overall strategy for the RR SMR commissioning programme is presented in E3S Case Chapter 14: Plant Construction & Commissioning, Reference [12].

7.5.9 ALARP in Design Development

The design of the AMS [JRQ] has been developed in accordance with the systems engineering design process, which includes alignment to RGP & 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 E3S criteria (as described in PSCR Chapter 3: E3S Objectives & Design Rules, Reference [6]).

Discussion on the development of the overall C&I architecture to reduce risks to ALARP is presented in Section 7.1.6.

7.5.10 Ongoing Design Development

The RR SMR design definition is currently in development as described in Section 7.0.2. All design development risks and opportunities are captured and managed by design teams. Further details of design development will be incorporated into a future revision of the E3S Case as evidence in the CAE Route Map becomes available.

7.6 C&I Essential Support Systems

The RR SMR C&I systems rely upon and provide control and monitoring of essential Reactor Island support services, failure of which can result in the unavailability of C&I systems providing a Safety Measure. In such cases, 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 still being developed, and are expected to include:

1. HVAC
2. Electrical power distribution

Public – Not Listed – Not Subject to Export Controls

7.7 Human Machine Interface

7.7.1 Main Control Room

The MCR is the primary location for the control and management of activities related to the reactor and power generation located within Reactor Island [R01] inside the Hazard Shield. It will be design in accordance with Human Factors requirements, as described in E3S Case Chapter 18: Human Factors Engineering, Reference [13].

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] for safety important functions sufficient to shut-down the reactor and to monitor and maintain it in a safe state.

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

1. To take pre-planned manual actions to bring the plant to a safe state

2. To determine whether the FSFs are being fulfilled

3. 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)

4. 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

5. To determine the need to initiate action to protect the public from a release of radioactive material

6. To implement the SAMGs at the plant

7.7.2 Supplementary Control Room

The SCR is located within Reactor Island [R01] outside of the Hazard Shield. The SCR is used to control and monitor aspects of the reactor and associated systems if the MCR is evacuated.

The SCR does not replicate full MCR functionality, however, provides sufficient control and instrumentation to manage plant operations so that the reactor can be placed and maintained in a shutdown state, residual heat can be removed, and the essential plant variables can be

monitored should there be a loss of ability to perform these essential safety functions in the MCR.

To provide effective monitoring and control of the facility in faults and accident conditions, the RPS [JRA], DPS [JQA] and AMS [JRQ] interfaces in the SCR are assumed to be essentially identical to those in the MCR. A normal operator workstation position is also assumed, though large wall displays and multiple operator workstations are not required as there is no intention to perform normal operations from the SCR.

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.

7.7.3 Emergency Control Centre

An ECC is provided on-site, located within Reactor Island [R01] outside of the Hazard Shield. The ECC is used to co-ordinate activities in response to emergencies such as fires or radiation emergencies and is not permanently staffed.

The ECC will include facilities such as Closed-Circuit Television (CCTV), Information Technology (IT), communication equipment and Personal Protective Equipment (PPE) such as dosimeters. The ECC will include the ability to monitor plant status (via normal operator interfaces) but no control capabilities will be provided.

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

7.7.4 Technical Support Centre

A Technical Support Centre (TSC) is also located within Reactor Island [R01] outside of the Hazard Shield and is staffed by technical engineers who support the MCR operators during abnormal operations.

The TSC will include facilities such as IT, communications equipment, and display of parameters shown in the MCR via normal operator interfaces. The TSC concept is to be developed further as the design is developed.

7.7.5 Off-Site Emergency Control Centre

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

The Off-Site ECC will likely include IT and communications equipment and is likely to display key parameters from the power station. The Off-Site ECC concept is to be developed further as the design is developed, including multi-unit site and fleet considerations.

7.7.6 ALARP in Design Development

The design of HMIs in the control rooms and procedures used to verify and validate the functional design are based on RGP, including IEC 60964, Reference [8], and IEC 60965, Reference [9].

Hardwired and computerised HMIs have been considered for the RR SMR, with the PCD design baseline selecting an HMI solution that is predominantly computerised that has a robust hardwired back-up for a sub-set of important safety displays and controls.

This option has been selected following an extensive review of RGP and OPEX from other Pressurised Water Reactor (PWR) designs, and is considered to maintain DiD and achieve required reliabilities as it includes both RPS operator terminals and Class 1 DPS controls and displays in both the MCR and SCR.

The design also represents a simplified solution compared to a full hardwired back-up system, which is consistent with RGP seen on other PWR designs, noting that different solutions are adopted dependent on national regulations, including both full and minimal hardwired back-up HMIs.

Public – Not Listed – Not Subject to Export Controls

7.8 Conclusions

7.8.1 Conclusions

Preliminary evidence is presented to support the overall chapter claim that 'The RR SMR C&I is designed and substantiated to achieve functional and non-functional safety requirements through the lifecycle and reduce risks to As Low As Reasonably Practicable', which contributes to the overall E3S objective to protect people and the environment from harm.

The overall C&I architecture is developed based on non-functional system requirements derived from UK and international RGP and OPEX, designed 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 to support reduction of risks to ALARP.

The PCD architecture is presented for the RPS [JRA], DPS [JQA], AMS [JRQ], and RPCMS [JS]. Further work is required to develop the design of each system, including requirements definition and traceability to the Fault Schedule, detailed design definition, and ultimately verification of safety requirements. SSCs excluded from this revision based on limited maturity, as described in Section 7.0.2, will be incorporated as their design is matured.

The full suite of underpinning evidence will be developed in line with CAE Route Map and reported in future revisions of the E3S Case.

7.8.2 Assumptions & Commitments on Future Dutyholder

None identified at this revision.

7.9 References

[1] RR SMR Report, SMR0004294/001, “E3S Case Chapter 1: Introduction,” March 2023.
[2] RR SMR Report, SMR0002155/001, “E3S Case Route Map,” March 2023.
[3] RR SMR Report, SMR0003977/001, “E3S Case Chapter 15: Safety Analysis,” March 2023.
[4] RR SMR Report, SMR0000670/001, “Reactor Controls and Instrumentation - JY System Outline Description,” June 2022.
[5] RR SMR Report, SMR0000510/001, “Rolls-Royce SMR C&I Engineering Schedule,” June 2022.
[6] RR SMR Report, SMR0004589/001, “E3S Case Chapter 3: E3S Objectives & Design Rules,” March 2023.
[7] RR SMR Report, SMR0003771/001, “E3S Case Chapter 6: Engineered Safety Features,” March 2023.
[8] British Standard BS IEC 60964, “Nuclear Power Plants- Control Rooms - Design,” December 2019.
[9] British Standard BS IEC 60965, “Nuclear Power Plants- Control Rooms - Supplementary control room for reactor shutdown without access to main control room,” February 2016.
[10] British Standard BS EN IEC 61226, “Nuclear Power Plants – Instrumentation and Control Important to Safety- Classification of Instrumentation and Control Functions,” September 2009.
[11] RR SMR Report, SMR0000465/001, “Outline V&V Plan for C&I Systems,” June 2022.
[12] RR SMR Report, SMR0004289/001, “E3S Case Chapter 14: Plant Construction & Commissioning,” March 2023.
[13] RR SMR Report, SMR0004520/001, “E3S Case Chapter 18: Human Factors Engineering,” March 2023.
[14] British Standard BS IEC 61513, “Nuclear Power Plants - Instrumentation and Control Important to Safety - General Requirements for Systems,” August 2011.

7.10 Appendix A: CAE Route Map

7.10.1 Chapter 7 Route Map

A preliminary Claims decomposition from the overall Chapter 7 Claim is summarised in Table 7.10-1, including the Tier 2 Evidence underpinning the Claims at PCD (i.e. summarised in Revision 1 of this report) and further Tier 2 Evidence still to be developed.

Table 7.10-1: CAE Route Map

Level 1 Claims	**Level 2 Claims**	**Level 3 Claims**	**Arguments**	**Evidence Summary within Chapter 7**	**Underpinning Tier 2 Evidence** ***at PCD***	**Underpinning Tier 2 Evidence** ***in development***
The C&I systems provide the required safety functions	The C&I Safety Functional Requirements are derived and justified based on sound safety principles and methods	-	A comprehensive set of functional requirements are derived in the safety analysis (Fault Schedule), placed on Structures, Systems & Components, based on functions to be delivered during Plant States Design Basis Condition (DBC)-1 to DBC-5, with C&I functions carried forward to the C&I Engineering Schedule	Section 7.1.2	DOORS Reactor Island Control & Protection [JY] Requirements Module	C&I Engineering Schedule

Level 1 Claims	Level 2 Claims	Level 3 Claims	Arguments	Evidence Summary within Chapter 7	Underpinning Tier 2 Evidence *at PCD	Underpinning Tier 2 Evidence *in development
	The Overall C&I Architecture assigns the required safety functions to individual C&I Systems	The DPS [JQA] provides the required safety functions	-	Not applicable (n/a)	n/a	System Outline Descriptions for each individual C&I system
		The RPS [JRA] provides the required safety functions	-			
		The AMS [JRQ] provides the required safety functions	-			
		The RPCS [JSA] provides the required safety functions	-			
The C&I systems incorporate the required non-functional system requirements	Non-functional system requirements are derived and justified based on sound safety principles and methods	-	Non-functional requirements for C&I are derived based on the E3S principles, IECs and British Standards	Section 7.1.2	DOORS Reactor Island Control & Protection [JY] Requirements Module	DOORS Reactor Island Control & Protection [JY] Requirements / Definition Modules

Level 1 Claims	Level 2 Claims	Level 3 Claims	Arguments	Evidence Summary within Chapter 7	Underpinning Tier 2 Evidence *at PCD	Underpinning Tier 2 Evidence *in development
	The Overall C&I Architecture allocates the required non-functional system requirements to individual C&I Systems	C&I systems apply appropriate Defence-in-Depth	-	Section 7.1.2	Reactor Island Control & Protection [JY] System Outline Description, Reference [4]	System Outline Descriptions for each individual C&I system
		C&I systems employ a suitable approach for prioritisation of shared demands on actuation	-	Section 7.1.5		
		C&I systems are appropriately classified in accordance with their safety significance	-	Section 7.1.3		
		C&I systems incorporate suitable independence	-	Section 7.1.2		
		C&I systems incorporate suitable diversity	-			

Level 1 Claims	Level 2 Claims	Level 3 Claims	Arguments	Evidence Summary within Chapter 7	Underpinning Tier 2 Evidence *at PCD	Underpinning Tier 2 Evidence *in development
		C&I systems incorporate suitable levels of redundancy to achieve the single failure criterion	-			
		C&I systems achieve the required reliability	-			
		C&I systems demonstrate suitable failure behaviour	-			
		C&I systems include provisions for testing and maintainability	-			
		C&I systems facilitate EMIT and ageing management	-			

Level 1 Claims	Level 2 Claims	Level 3 Claims	Arguments	Evidence Summary within Chapter 7	Underpinning Tier 2 Evidence *at PCD	Underpinning Tier 2 Evidence *in development
		C&I systems are qualified and can withstand Internal & External Hazards	-			
		C&I systems incorporate appropriate HMIs	-	Section 7.7		
		C&I systems are sufficiently robust against cyber attacks	-	Not applicable, to be covered in GSR		

Level 1 Claims	Level 2 Claims	Level 3 Claims	Arguments	Evidence Summary within Chapter 7	Underpinning Tier 2 Evidence *at PCD	Underpinning Tier 2 Evidence *in development
C&I architecture is designed to achieve safety requirements, considering RGP & OPEX to reduce risks to ALARP	-	-	The preferred design solution has been designed according to an appropriate process, following a structured systems engineering approach in accordance with IEC61513, Reference [14], development life cycle with evaluation against safety criteria supporting the decision-making process	Section 7.1.6 Sections 7.2.9, 7.3.9, 7.4.9, 7.5.9	Reactor Island Control & Protection [JY] System Outline Description, Reference [4]	System Outline Descriptions for each individual C&I system

7.11Acronyms and Abbreviations

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
CCTV	Closed-Circuit Television
CoFT	Control of Fuel Temperature
CoR	Control of Reactivity
CoRM	Confinement of Radioactive Material
DBA	Design Basis Accident
DBC	Design Basis Condition
DEC	Design Extension Condition
DiD	Defence-in-Depth
DMZ	De-Militarized Zone
DOORS	Dynamic Object-Oriented Requirements System
DPS	Diverse Protection System
E3S	Environment, Safety, Security & Safeguards
ECC	Emergency Control Centre
EMC	Electro-Magnetic Compatibility
EMIT	Examination, Maintenance, Inspection & Testing
EOP	Emergency Operating Procedure
FSF	Fundamental Safety Function
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
IEC	International Electrotechnical Commission
IT	Information Technology
MCR	Main Control Room
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	Pre-Construction Safety Report
PFD	Probability of Failure on Demand
PIE	Postulated Initiating Event
PPE	Personal Protective Equipment
PSA	Probabilistic Safety Assessment
PWR	Pressurised Water Reactor
RCS	Reactor Control System
RD	Reference Design
RGP	Relevant Good Practice
RLPPS	Reactor Limitation & Preventive Protection System
RPCMS	Reactor Plant Control & 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
SSC	Structure, System and Component
TSC	Technical Support Centre
UK	United Kingdom
V&V	Verification and Validation
Y	Yes