Office for Nuclear Regulation

An agency of HSE

ASSESSMENT REPORT

Civil Nuclear Reactors Programme

NNB GenCo Ltd: Hinkley Point C Pre-Construction Safety Report 2012 – Assessment Report for Control and Instrumentation Workstream

Assessment Report: ONR-CNRP-AR-13-103
Revision 0
Version 2
21 March 2014

COPYRIGHT

EXECUTIVE SUMMARY

This assessment report reviews that part of the Hinkley Point C Pre-Construction Safety Report 2012 (HPC PCSR2012) that falls within the scope of the Office for Nuclear Regulation's (ONR) control and instrumentation (C&I) workstream. Most of this material lies in HPC PCSR2012 chapter 7, specifically sub-chapters 7.1 to 7.7, which have been reviewed. In addition, this assessment has reviewed the C&I aspects of sub-chapters 10.2, 10.3 and 12.3, respectively, to determine how HPC PCSR2012 has dealt with systems outside the scope of ONR's Generic Design Assessment (GDA).

A final version of the GDA Pre-Construction Safety Report (PCSR) issued in November 2012 formed the basis for issue by ONR on 13 December 2012 of a Design Acceptance Confirmation (DAC) for the UK EPR™ design. The GDA PCSR addressed only the key elements of the design of a single UK EPR™ unit (the generic features on "the nuclear island") but excluded ancillary installations that a potential purchaser of the design could select after taking the site location into account. Certain matters were also deemed to be outside the scope of the GDA PCSR.

In contrast HPC PCSR2012 addresses the whole Hinkley Point C (HPC) licensed site comprising the proposed twin UK EPR™ units and all ancillary installations. Some matters that were outside the scope of GDA PCSR are also addressed in HPC PCSR2012. As the generic features were addressed in the GDA process, my focus has been on the limited site-specific documentation that has not been formally assessed by ONR previously. The remaining, generic documentation has been copied into PCSR2012 from an earlier March 2011 GDA PCSR but this has now been superseded by the November 2012 GDA PCSR report. .

It is important to note that HPC PCSR2012 alone is not sufficient to inform a future ONR decision on whether to permission construction of HPC. NNB GenCo Ltd intends to submit a major revision to HPC PCSR2012 before seeking consent from ONR for Nuclear Island construction which will fully integrate the final GDA PCSR and will be supported by other documentation

Based on my assessment, I am not satisfied that the claims, arguments and evidence laid down within PCSR2012 are at this time sufficient to support permissioning of the C&I safety systems and equipment intended for use at HPC. This is due to the incomplete nature of the information in the PCSR on the design and the ongoing development of a number of C&I safety systems and equipment being developed to fulfil the GDA outcomes. NNB GenCo Ltd also need to provide more information on those systems and equipment important to safety that are associated with the balance of plant outside the scope of GDA.

However, it is acknowledged that a number of the shortfalls identified in my assessment report have already been raised with NNB GenCo Ltd so that they can be addressed as part of the design and development of the C&I safety systems covered in the PCSR. On other matters identified in my report I have raised a Level 3 Issue as an entry on the ONR Issues database, on those shortfalls that have not been specifically addressed by actions assigned to NNB GenCo Ltd to date. This primarily covers the limited information in PCSR2012 on standards compliance, equipment qualification procedures, protective measures for adverse electromagnetic phenomena and design for reliability of C&I safety systems and equipment important to safety at HPC, which are outside the scope of GDA.

Judged against my expectations for a PCSR to support a consent from ONR, I consider that HPC PCSR2012 should be recorded in the Integrated Intervention Strategy (IIS) database with a rating of 4 (Yellow), below standard. This is in recognition that PCSR2012 is considered to require further work as outlined above.

LIST OF ABBREVIATIONS

AF	Assessment Finding
AMS	Aeroball Measuring System
BDR	Basic Design Reference
BMS	(ONR) How2 Business Management System
C&I	Control and Instrumentation
CINIF	C&I Nuclear Industry Forum
COT	Core Outlet Thermocouples
CVCS	Chemical and Volume Control System
DAC	Design Acceptance Confirmation
EMI	Electromagnetic Interference
FA3	Flammanville 3 (nuclear power station)
FMECA	Failure Mode, Effects and Criticality Analysis
GDA	Generic Design Assessment
HPC	Hinkley Point C (nuclear power station)
HSE	Health and Safety Executive
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
ICBM	Independent Confidence Building Measure
IIS	Integrated Intervention Strategy
LC	Licence Condition
LOOP	Loss Of Offsite Power
MSSS	Main Steam Supply System
NCSS	Non-Computerised Safety System
NSS	Nuclear Sampling System
ONR	Office for Nuclear Regulation (an agency of HSE)
PCSR	Pre-construction Safety Report
PICS	Process Information and Control System
PIPS	Process Instrumentation Pre-processing System
PRMS	Plant Radiation Monitoring System
PS	Protection System
PSOT	Protection System Operator Terminal
PSR	Preliminary Safety Report
QA	Quality Assurance

LIST OF ABBREVIATIONS

QDS	Qualified Display System
RCCA	Rod Control Cluster Assemblies
RCP	UKEPR™ system code for the Reactor Coolant System (RCS)
RCS	Reactor Coolant System
RCSL	Reactor Control, Surveillance and Limitation system
RGP	Relevant Good Practice
RD	Responsible Designer
RP	Requesting Party
RPI	Rod Position Instrumentation
RPVDT	Reactor Pressure Vessel Dome Theromcouples
RPVL	Reactor Pressure Vessel Level
RRC-B	Risk Reduction Category B
SA	Severe Accident
SAP	Safety Assessment Principle(s) (HSE)
SAS	Safety Automation System
SFAIRP	So far as is reasonably practicable
SG	Steam Generator
SICS	Safety Information and Control System
SPND	Self Powered Neutron Detectors
SSC	System, Structure and Component
TAG	Technical Assessment Guide(s) (ONR)
TSC	Technical Support Contractor
UKEPR™	United Kingdom European Pressurised Reactor
UPS	Uninterruptible Power Supply
WENRA	Western European Nuclear Regulators' Association

TABLE OF CONTENTS

Tables

1 INTRODUCTION

1.1 Background

1 This report presents the findings of my assessment of that portion of the Hinkley Point C Pre-Construction Safety Report 2012 (HPC PCSR2012) (Ref.1) that falls within the scope of the control and instrumentation (C&I) workstream.

2 Assessment was undertaken in accordance with the requirements of the Office for Nuclear Regulation (ONR) How2 Business Management System (BMS) procedure AST/003 (Ref. 2). The ONR Safety Assessment Principles (SAP) (Ref.3) together with supporting Technical Assessment Guides (TAGs) (Ref. 4) have been used as the basis for this assessment.

3 This assessment report (AR) has been written to support a summary assessment report that addresses whether HPC PCSR2012 demonstrates suitable progress towards meeting ONR's requirements for an adequate Pre-Construction Safety Report. To this end this AR provides information on matters that should be addressed in the next revision of HPC PCSR. To achieve this end I have raised a Level 3 Issue on matters that are required to be addressed by NNB GenCo Ltd before the next revision of the HPC PCSR3.

1.2 Scope

4 The scope of this report covers the C&I workstream and most of the material relevant to this assessment is provided in HPC PCSR2012 chapter 7 and I have therefore reviewed the material in sub-chapters 7.1 to 7.7. In addition, I have also reviewed the C&I aspects of sub-chapters 10.2, 10.3 and 12.3 to determine how PCSR2012 has dealt with systems that were outside the scope of GDA.

5 A final version of the Generic Design Assessment (GDA) Pre-Construction Safety Report (PCSR) issued in November 2012 formed the basis for issue by ONR on 13 December 2012 of a Design Acceptance Confirmation (DAC) for the UK EPR™ design. The GDA PCSR addressed only the key elements of the design of a single UK EPR™ unit (the generic features on "the nuclear island") but excluded ancillary installations that a potential purchaser of the design could select after taking the site location into account. Certain matters were also deemed to be outside the scope of the GDA PCSR.

6 In contrast HPC PCSR2012 addresses the whole Hinkley Point C (HPC) licensed site comprising the proposed twin UK EPR™ units and all ancillary installations. Some matters that were outside the scope of GDA PCSR are addressed in HPC PCSR2012. As the generic features were addressed in the GDA process, I have concentrated my attention on site-specific documentation that has not been formally assessed by ONR previously. The remaining, generic documentation has been copied into PCSR2012 from an earlier March 2011 GDA PCSR but this has now been superseded by the November 2012 GDA report. I have only revisited the generic documentation if recent developments have materially affected the case being made.

7 It is important to note that HPC PCSR2012 alone is not sufficient to inform a future ONR decision on whether to permission construction of a nuclear power plant at HPC and NNB GenCo Ltd intends to submit other supporting documentation. It should also be noted that HPC PCSR2012 will be superseded by a further site-specific revision intended to fully reflect the final GDA PCSR and other design changes from Flamanville 3 (FA3) which is the reference design for HPC.

8 In addition, it should be noted that the approach to safety function categorisation and safety system classification agreed during GDA is not fully reflected in HPC PCSR2012

which largely uses the approach employed on FA3. The integration of the methodology (Ref. 5) agreed during GDA should be demonstrated in the next revision of HPC PCSR.

1.3 Methodology

9 The methodology for the assessment follows the requirements of the ONR Business Management System (BMS) 'produce assessments' step in the nuclear safety permissioning process and Ref. 2 in relation to the mechanics of assessment.

2 ASSESSMENT STRATEGY

10 My assessment strategy is set out in this section. This identifies the scope of the assessment and the standards and criteria that have been applied.

2.1 Standards and Criteria

11 The relevant standards and criteria I have adopted for this assessment are principally the Safety Assessment Principles (SAP) (Ref. 3), internal ONR Technical Assessment Guides (TAG) (Ref. 4), relevant national and international standards and relevant good practice informed from existing practices adopted on UK nuclear licensed sites. The key SAPs and relevant TAGs are detailed within this section. I have referenced national and international standards and guidance where appropriate within my assessment report. I have also cited relevant good practice, where applicable, within the body of my assessment report.

2.2 Safety Assessment Principles

12 I have listed the key SAPs[1] applied within the assessment in Table 1 of this report.

2.2.1 Technical Assessment Guides

13 The following Technical Assessment Guides have been used as part of this assessment (Ref. 4):

- T/AST/003 Issue 6.
- NS-TAST-GD-015 Revision 1.
- NS-TAST-GD-019 Revision 2.
- NS-TAST-GD-046 Revision 3.

2.2.2 National and International Standards and Guidance

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

- BS EN 61226:2010 (Ref. 21).
- BS EN 61513: 2013 (Ref. 7).

2.3 Use of Technical Support Contractors

15 No Technical Support Contractors have been used in this assessment.

[1] The SAPs referred to in this report are derived from a HSE document entitled "Safety Assessment Principles for Nuclear Facilities – Subset for NP&E assessment" (Ref. 6).

2.4 Integration with other Assessment Topics

16 No integration with other topics has been necessary to support my C&I assessment of HPC PCRS2012.

2.5 Out-of-scope Items

17 Not applicable.

3 LICENSEE'S SAFETY CASE

3.1 HPC PCSR2012 Material Assessed

18 The majority of material relating to the C&I Workstream is located in Chapter 7[2], specifically in sub-chapters 7.1 to 7.7.

19 The sub-chapters considered as part of this assessment cover the following topics:

- design principles of the instrumentation and control (I&C) systems (Ref. 8).
- general architecture of the I&C systems (Ref. 9).
- Class 1 I&C systems (Ref. 10).
- Class 2 I&C systems (Ref. 11).
- Class 3 I&C systems (Ref. 12).
- instrumentation (Ref. 13).
- I&C tools, development process and substantiation (Ref. 14).

20 Other material is contained in sub-chapters 10.2, 10.3 and 12.3, which cover:

- turbo generator set (Ref. 15)3.
- main steam system (Ref. 16)6.
- radiation protection measures (Ref. 17)6.

21 These sub-chapters, with the exception of sub-chapter 10.2, were all published and approved by EDF DIN CNEN and AREVA in their combined role as GDA Requesting Party (RP) for the UKEPR™ during its GDA. This information also forms an important part of the development of HPC PCSR2012 by NNB GenCo Ltd where EDF DIN CNEN are acting as the Responsible Designer (RD) for HPC.

22 The sub-chapters were approved for publication between 27 March 2011 and 6 November 2012 as part of NNB GenCo Ltd's consolidated PCSR update programme and their contents align with information provided to ONR in March 2011 as a GDA PCSR with some updates that reflect progress made in GDA. I understand that the information will be further updated to align with ONR's expectations at the end of GDA.

23 The following sections provide a brief summary of the contents of the above sub-chapters and the Licensee's safety case.

---

[2] Chapter 7 of PCSR2012 is entitled Instrumentation and Control.

[3] Refs. 14 and 15 form part of Chapter 10: Steam and power conversion systems whilst Ref. 16 forms part of Chapter 12: Radiation protection.

3.1.1 Sub-chapter 7.1 - Design principles of the I&C[4] Systems (Ref. 8)

24 This sub-chapter as part of HPC PCSR2012 outlines the basic design principles for C&I systems used on the UKEPR™ to be constructed at HPC and generically describes the main safety functions. It states that functional categorisation and classification criteria applicable to C&I systems will be performed in accordance with the methodology given in sub-chapter 3.2[5].

25 Sub-chapter 7.1 describes in general terms the requirements relating to the design of C&I systems, including an interpretation of single failure criterion, an outline of the basis for qualification and testing of the C&I systems, periodic testing and relevant standards. In particular, specific reference is made to compliance with the requirements of RCC-E[6] and relevant standards, although no specific standards are stated.

26 A description is provided of the design basis for the C&I system architecture organised into a four level structure (i.e. Levels 0, 1, 2 and 3 as outlined in 3.1.2 below), which determines the interaction of the systems and the types of function that they perform.

27 A brief description is given for the concept of defence in depth that has been applied to C&I-based safety systems, which has been established to meet deterministic safety criteria and the results of probabilistic analysis. Sub-chapter 7.1 states that the C&I architecture should be configured to ensure that sufficient independence is provided between lines of defence to achieve the probabilistic targets for the UKEPR™ as set out in Chapter 15 (Probabilistic Safety Assessment) of PCSR2012.

28 A simple prioritisation scheme is set out for the actuation of protection and control actions to avoid any adverse consequences as a result of contradictory commands within the safety functions. These design rules operate on the basis of a defined order of system and manual command priory in accordance with the classification of relevant systems (highest class has the highest priority).

29 Sub-chapter 7.1 sets out development lifecycle requirements for the design of C&I safety systems, which aligns with the RD's engineering processes, and has features in common with the C&I safety lifecycle set out in BS EN 61513 (Ref. 7).

3.1.2 Sub-chapter 7.2 - General architecture of the I&C systems (Ref. 9)

30 This sub-chapter describes the overall architecture of the C&I safety systems and the qualification principles that are proposed for systems, equipment and components, including software. A three level C&I architecture is set out as:

- Level 0: process interfaces (e.g. sensors, transducers, process information pre-processing system (PIPS), switchgear, and priority actuation and control system (PACS)).

[4] NNB GenCo Ltd, as the licensee, and its RD refer to this workstream as Instrumentation and Control (I&C) rather than Control and Instrumentation (C&I), which is preferred discipline description within ONR. This report uses C&I with the exception of the licensee's document titles and other references.

[5] It should be noted that the methodology referred to in sub-chapter 3.2 is an earlier revision of Ref.5.

[6] RCC-E (Ref. 18) is a technical code for electrical equipment that is published by AFCEN, which is based on both international and French standards, that covers C&I equipment. PCSR2012 refers to the 12/2005 edition of RCC-E which was superseded in 2012.

- Level 1: automation systems (e.g. protection system (PS), safety automation system (SAS) and non-computerised safety system (NCSS)).
- Level 2: monitoring and control systems (e.g. data processing for monitoring and control of processes implemented in process information and control system (PICS) and safety information and control system (SICS), interfaces to the protection system operator terminal (PSOT), and the severe accident panel).
- Level 3: non real-time applications (e.g. data acquisition).

31 A table provides a description of the relationship between system classification and claimed reliability for a number of the C&I safety systems described in sub-chapters 7.3 (Ref. 10), 7.4 (Ref. 11) and 7.5 (Ref. 12). The claims are made for Class 1 safety systems at $1x10^{-4}$pfd, for Class 2 at $1x10^{-3}$pfd (NCSS only) otherwise at $1x10^{-2}$pfd and Class 3 at $1x10^{-1}$pfd.

32 In addition, a comprehensive list is provided of the C&I safety systems and equipment at each level in the architecture with a brief description of relevant safety functions. This listing focuses largely on those C&I safety systems and equipment covered by chapter 7 and its sub-chapters. A description is also given of the measures that are to be applied to ensure independence and diversity within each level of the architecture.

33 Sub-chapter 7.2 briefly outlines the proposed arrangement of the divisional structure of C&I safety systems and equipment in terms of the rooms, cubicles and cabling allocated at HPC. This also covers by reference to PCSR2012 sub-chapters 8.4 (electrical supply and layout – specific design principles) and 9.4 (heating, ventilation and air conditioning systems) the environmental conditions in these rooms.

34 An outline of the qualification principles and processes is given in this sub-chapter, which includes a section on the relationship between qualification and the development lifecycle. The qualification processes for C&I safety systems involve factory (referred to as product line) and plant-specific qualification based on tests, analysis and the use of operating experience.

3.1.3 Sub-chapter 7.3 - Class 1 I&C systems (Ref. 10)

35 This sub-chapter as part of HPC PCSR2012 outlines the basic design principles for C&I systems used at the UKEPR™ that have been classified as Class 1 that perform Category A functions. In particular, the document describes the safety functions and design requirements applicable to:

- Protection System (PS)
- Safety Information and Control System (SICS)

36 Sub-chapter 7.3 provides details on the design basis and architecture for each of the above Class 1 systems and outlines the interfaces with other C&I safety systems. Details are also provided on the dual power supply arrangements for these systems based on a combination of supplies derived from ac and dc sources within the power plant to form an uninterruptible power supply. Information is also provided on the back-up emergency power supply arrangements for these systems based on supplies derived from emergency diesel generators within the power plant.

37 Both of the above Class 1 systems implement functions that have been assigned as Category A, B and C.

38 The PS is claimed to be based on digital electronic technology that uses software in the form of a Teleperm XS[7] platform. SICS is reported as being based on digital electronic technology that does not use software. Details of the type of digital electronic technology(ies) to be used in the construction of SICS are not stated in the sub-chapter.

39 Sub-chapter 7.3 outlines the proposals for maintenance and testing of the above Class 1 systems using a combination of service units and self-test features. The test equipment is to be designed to meet the requirements of Class 2 and, if this is not possible, compensatory measures are to be applied.

3.1.4 Sub-chapter 7.4 - Class 2 I&C systems (Ref. 11)

40 This document as part of HPC PCSR2012 outlines the design principles for C&I systems used at the UKEPR that have been classified as Class 2 that perform Category B functions and may act as a diverse line of protection for those systems that perform Category A functions. In particular, the document describes the safety functions and design requirements applicable to:

- Safety Automation System (SAS)
- Reactor Control, Surveillance and Limitation (RCSL) system
- Non-Computerised Safety System (NCSS)

41 The document provides details on the design basis and architecture for each of the above Class 2 systems and outlines the interfaces with other C&I safety systems. Information is also provided on the dual power supply arrangements for these systems based on a combination of supplies derived from ac and dc sources within the power plant to form an uninterruptible power supply. Sub-chapter 7.4 provides information on the back-up emergency power supply arrangements for these systems based on supplies derived from emergency diesel generators within the power plant.

42 The SAS is claimed to be based on digital electronic technology that uses software in the form of a SPPA-T2000[8] platform. Similarly, RCSL is also based on digital electronic technology that uses software in the form of the Teleperm XS platform.

43 The NCSS is claimed to be based on non-computerised technology in the form of a Unicorn[9] platform, which is implemented on a series of non-computerised modules. The non-computerised technology is being developed using magnetic logic and photoMOS[10] technologies (Ref. 19).

44 Sub-chapter 7.4 also provides information on the provisions for periodic testing for each of the above systems on the basis of end-to-end proof test principles for individual channels

[7] Teleperm XS is an AREVA product name.

[8] SPPA T2000 is a product name for a class of Siemens automation systems.

[9] Unicorn is an AREVA product name.

[10] PhotoMOS technology refers to form of semiconductor device that typically contains one or more metal oxide semiconductor field effect transistors (MOSFET). PhotoMOS devices such as solid state relays are commonly used in a wide range of industrial applications.

from sensor through to change of state of the actuator(s). It is noted that any equipment used to test the Class 2 safety systems will be designed to be at least Class 3.

3.1.5 Sub-chapter 7.5 - Class 3 I&C systems (Ref. 12)

45 This document as part of HPC PCSR2012 outlines the basic design principles for C&I systems used at the UKEPR that have been classified as Class 3 that perform Category C functions. The document also covers systems and equipment that perform functions associated with a Loss Of Offsite Power (LOOP) severe accident scenario. In particular, the document describes the safety functions and design requirements applicable to:

- Risk Reduction Category B (RRC-B) SAS
- Process Information and Control System (PICS)
- Process Automation System (PAS)
- Severe Accident I&C system (SA I&C) system

46 Sub-chapter 7.5 provides details on the design basis and architecture for each of the above Class 3 systems and outlines the interfaces with other C&I safety systems. Details are also provided on the dual power supply arrangements for these systems based on a combination of supplies derived from ac and dc sources within the power plant. Information is also provided on the emergency power supply arrangements for these systems based on a combination of supplies derived from relevant emergency and ultimate diesel generators within the power plant.

47 The document states that the SA I&C system will be supplied by redundant battery-backed uninterruptible power supply (UPS) systems that have a 12-hour capacity. This arrangement is provided to compensate for the LOOP scenario.

48 The RRC-B SAS, PICS and PAS are reported as being based on digital electronic technology that uses software in the form of a SPPA-T2000 platform. Similarly, SA I&C is also based on digital electronic technology that uses software in the form of the Teleperm XS platform.

49 It is reported that the single failure criterion does not apply to the above Class 3 safety systems, with the exception of PICS equipment that is to form the operator workstation equipment in the Main Control Room that is subject to the requirements applicable to Class 2 safety systems.

50 The document also states that periodic testing of each of the above systems is to be performed and that the systems will be designed accordingly. No specific information is provided on the test principles that may be applied to the above Class 3 safety systems with the exception of SA I&C that is proposed to use overlapping tests to ensure that all parts of the system are tested at a frequency determined by a probabilistic safety assessment.

3.1.6 Sub-chapter 7.6 - Instrumentation (Ref. 13)

51 Sub-chapter 7.6 as part of HPC PCSR2012 outlines the basic design principles for instrumentation used at the UKEPR™ that are involved in three main safety functions, namely: control of fuel reactivity, fuel heat removal and confinement of radioactive material.

52 The instrumentation also measures those parameters (pressure, flow, level, temperature, speed, actuator position, and neutron flux) required by various process control systems and to inform operators about the status of the plant.

53 The instrumentation covered by Sub-chapter 7.6 will generally have 4 to 20 mA[11] output signals and those devices classified for use in safety functions will be appropriately qualified for their intended use. Also, the document outlines generic requirements for equipment selection, use and calibration.

54 The document states that when used to implement a safety or safety-related function(s) the avoidance of smart[12] instrumentation equipment is preferred.

55 Descriptions of safety classified instrumentation are provided in terms of measurement of pressure, flow, liquid level, temperature, rotational speed, voltage, frequency and main steam safety valve position. The descriptions provided give a general indication of the means that may be used to measure each parameter without specific details of the characteristics of the equipment used. There is for a number of the above parameters (e.g. pressure, temperature and flow) a selection of the types of equipment that may be used (e.g. thermocouples or resistance temperature detectors for temperature measurement).

56 Accident and severe accident instrumentation are described in terms of general principles that relate to monitoring concepts and functions. A description of typical provisions for process and environmental monitoring is given without specific details of claims made against the reliability of the monitoring systems where it may affect selection of instrumentation.

57 The document provides a section that describes the instrumentation requirements in relation to accident procedures in terms of permanent monitoring of six state functions, namely criticality of the core, Reactor Coolant System (RCS) pressure and temperature, RCP water inventory, Steam Generator (SG) integrity, SG water inventory and containment integrity. The document states that the relevant instrumentation should be capable of performing Category B functions.

58 A description is provided of the instrumentation that is claimed to be available for use during a severe accident in terms of dedicated actions, such as depressurisation of the primary system and injection of water onto the corium after transfer to the spreading area. This leads to two categories on instrumentation; the first covers those instruments required for operators to perform appropriate dedicated actions as part of Category C functions and other instruments that have been deemed as useful for monitoring severe accident progression.

59 Sub-chapter 7.6 describes a Process Instrumentation Pre-processing System (PIPS), which provides an interface between process instrumentation and safety systems based on the Teleperm XS platform that use their signals. The PIPS also distributes the same signals to other systems, such as SAS, and NCSS. The safety requirements applicable to PIPS are consistent with the highest safety category functions used in the UKEPR™.

60 In addition, the document describes in-core instrumentation that forms part of the following systems:

[11] 1/1000th of an ampere which is a measure of the flow of current in an electrical circuit.

[12] Smart instrumentation can be considered as a subset of smart devices which contain a microprocessor(s) or other forms of complex programmable electronic components that provide specific forms of functionality. Examples of smart devices can include pressure transmitters, valve positioners and some forms of electrical protection equipment.

- Aeroball Measuring System (AMS), which is an electromechanical computer-controlled instrumentation system, used to measure neutron flux distribution in the reactor core.
- Fixed in-core instrumentation comprising 72 Self-Powered Neutron Detectors (SPND), 36 Core Outlet thermocouples (COT) and 5 Reactor Pressure Vessel Dome Thermocouples (RPVDT).

61 The document describes the use of 12 instrumentation lances that are installed in the control assembly guide thimbles of fuel assemblies not occupied by control rod assemblies as the means of inserting the instrumentation into the core via penetrations in the reactor pressure vessel. The RPVDT are installed at different elevations in the upper dome by means of Reactor Pressure Vessel Level (RPVL) probes.

62 The fixed SPND instrumentation is reported to be Class 1 and supports functions up to Category A. The SPND measurement principle and configuration (12 radially distributed detector fingers each containing 6 SPNDs axially distributed over the reactor height) are described complete with functional characteristics.

63 The fixed COT instrumentation is reported to be Class 2 and supports functions up to Category B. The COT measurement principle and configuration (36 COT (3 thermocouples per in-core detector thimble) distributed over 12 measuring points) are described complete with functional characteristics.

64 The fixed RPVDT instrumentation is reported to be Class 2 and supports non-categorised functions, namely water temperature in the RPV dome. The RPVDT measurement principle and configuration is described without reference to functional characteristics.

65 The neutron detectors that form the ex-core instrumentation are reported to be Class 1 and supports functions up to Category A. The ex-core instrumentation measurement principle and configuration (separate instrumentation channel groups for source, intermediate and power range, respectively, up to 150% of the rated reactor power) are described complete with functional characteristics for each power range.

66 The Class 1 instrumentation associated with rod position measurement is described complete with interfaces to other systems, namely PS, RCSL, PICS and a Safety Information and Control system (SICS). The document outlines the design philosophy for the use of the rod position instrumentation in association with sub-banks of four Rod Control Cluster Assemblies (RCCA)[13], which forms a four-fold redundant structure when the RCCA sub-banks are moved together.

67 Sub-chapter 7.6 describes the means that will be used for surveillance of the rod positions on a continuous basis and in the course of reactor start-up routines. It is noted that periodic testing of rod position is not expected during normal operation.

68 The sub-chapter describes the instrumentation associated with a Reactor Pressure Vessel water Level (RPVL) measurement system that is intended for use post-accident to support operator decisions on mitigatory actions. The RPVL instrumentation is to comprise heated and unheated thermocouples, where the temperature difference between thermocouples is used to determine whether the coolant level in the reactor pressure vessel remains within pre-determined thresholds.

[13] There are 89 RCCA – 36 control rods and 53 shutdown rods – assigned to four divisions (i.e. position measurement of 22 rods per division). Note that one division also includes a central rod and has 23 rods..

69 A description of the RPVL equipment is provided complete with the design philosophy and details of its redundant architecture that monitors thresholds at the top, bottom and intermediate locations on each reactor pressure vessel hot leg. Operating and performance characteristics of the thermocouples are not specified in sub-chapter 7.6.

70 The sub-chapter briefly describes the instrumentation, namely accelerometers, that perform loose part and vibration monitoring functions. These accelerometers are non-classified equipment.

71 A Plant Radiation Monitoring System (PRMS) and its associated radiation protection instrumentation are also described in the sub-chapter in terms of a range of Category A safety functions. The instrumentation proposed to be used are a range of beta and gamma radiation detectors (see also 3.1.10 below).

72 Sub-chapter 7.6 also briefly describes the boron instrumentation used to monitor boron concentration in the Chemical and Volume Control System (CVCS) and Nuclear Sampling System (NSS), respectively. It is stated that the boron meter system has been assigned as Class 1 and performs a Category A function within the CVCS to mitigate the risk of incorrect boron concentration within the reactor coolant using four instrumentation channels.

73 The assigned Categorisation and Classification for the boron meter system when used as part of NSS is not stated in this sub-chapter or in the reference sub-chapter 9.3 (primary system auxiliaries).

74 The technology used in the construction of the boron meter system is not stated in this sub-chapter.

3.1.7 Sub-chapter 7.7 - I&C tools, development process and substantiation (Ref. 14)

75 Sub-chapter 7.7 provides information relevant to the design and development of the three platforms used by the C&I safety systems, namely Teleperm XS[10], SPPA-T2000[11] and Unicorn[12]. It also outlines the approach taken to design substantiation of those platforms that use software (Teleperm XS[10] and SPPA-T2000[11]), smart devices and any programmable electronic components that may be used in the UKEPR™.

76 The tools and development process used for programming of software-based C&I safety functions implemented by the Teleperm XS[10] platform have implications for a number of safety systems proposed to use this common platform, notably, PS, RCSL, SA I&C, and Rod Position Instrumentation (RPI). The PSOT is based on a Qualified Display System (QDS), which although a Teleperm XS product has its own specific design and configuration tools.

77 Sub-chapter 7.7 outlines the use of integrated tools used to program the Teleperm XS[10] platform to perform relevant safety functions as part of these C&I safety systems. The Teleperm XS[10] application software relevant to the UKEPR™ at HPC is proposed to be designed using a proprietary SPACE[14] engineering system whilst the QDS application software is designed the QDS design tool. These tools are able to perform a range of processes in terms of the productions and testing of the application software, including specification and hardware configuration, automatic code generation, verification and validation in simulation environments, and testing on C&I safety systems.

[14] SPACE is an acronym for Specification And Coding Environment.

78 The sub-chapter states that SPACE and QDS design tools will be developed using processes that will be commensurate with the availability and reliability requirements of the C&I safety systems. No specific availability and/or reliability claims are given but reference is made to the use of quality assurance plans, which forms an important aspect of safety management for software development.

79 The integrated tools and development process used for programming of software-based C&I safety functions implemented by the SPPA-T2000 platform have implications for a number of safety systems proposed to use this common platform, notably, SAS, PAS, RRC-B SAS and PICS. These tools, which are proposed to cover the lifecycle from design through to operation and future maintenance, are reported to be supported by administrative procedures to control software and hardware configuration changes. These administrative procedures are described at a high-level in the sub-chapter and it is stated that these will be provided as part of further documentation for a site-specific licence.

80 Similar to the Teleperm XS[10] design tools, the sub-chapter reports that those for the SPPA-T2000[11] platform, such as a CAD-based graphical programming tool, will be developed using processes that will be commensurate with the availability and reliability requirements of the C&I safety systems. No specific availability and/or reliability claims are given but reference is made to the use of quality assurance plans, which forms an important aspect of safety management for software development.

81 A detailed description is provided in sub-chapter 7.7 of the approach that is to be taken to the substantiation of software-based C&I safety systems in the form of production excellence and relevant independent confidence building measures (ICBMs), which aligns with the good practice outlined in NS-TAST-GD-046 (Ref. 4). The sub-chapter describes the basis for substantiation of each platform (i.e. Teleperm XS[10] and SPPA-T2000[11]) and the C&I safety systems that are to be implemented as part of UKEPR™. This includes details of relevant international standards and RCC-E (Ref. 18) and any independent assessment or reviews that are to be performed during design and development

82 Sub-chapter 7.7 also includes an overview of the approach proposed to be taken for the justification for use of smart devices that may be used as part of the UKEPR™, which is based on the use of production excellence and relevant ICBMs. It is stated that smart devices may be required as Class 1, 2 or 3 dependent upon the reliability claim made upon the system and the production excellence activities and relevant ICBMs will be graded accordingly.

3.1.8 Sub-chapter 10.2 – Turbo generator set (Ref. 15)

83 Sub-chapter 10.2, which was approved for publication on 24 April 2012 briefly outlines the turbo generator sets to be installed at HPC and at a high level covers protection to be provided for the generator and turbine, respectively.

84 The information provided relates to electrical protection only for the generator whilst turbine protection functions of overspeed and overpressure are outlined with insufficient detail to enable an assessment of their suitability for use at HPC. Also, there is no indication of whether turbine protection functions are to be used during post-trip sequences.

3.1.9 Sub-chapter 10.3 – Main steam system (safety classified part) (Ref. 16)

85 Sub-chapter 10.3, which was approved for publication on 30 March 2011, outlines the safety functions and design requirements applicable to the safety classified parts of the

Main Steam Supply System (MSSS). This includes a section on the C&I aspects of the four independent trains of the MSSS, which controls operation of essential actuators.

86 The classification of the C&I safety systems and equipment is not specified in sub-chapter 10.3 and although the general design requirements, such as the allocation to individual trains assigned to each steam generator, are described there is insufficient detail provided to enable an assessment of their suitability for use at HPC.

87 A description is provided of the application of the single failure criterion within the MSSS, which covers the C&I safety systems and equipment insofar as it states that a single failure should have no more effect on the steam system than a single failure of a MSSS component. There is no comment made in sub-chapter 10.3 in terms of common cause failure(s) that may need to be considered dependent upon the classification and relevant reliability claims, which are not specified (see above).

3.1.10 Sub-chapter 12.3 – Radiation protection measures (Ref. 17)

88 Sub-chapter 12.3 which was approved for publication on 27 March 2011, outlines the general design requirements (including radiation protection classification and zoning rules) and equipment installation rules for the PRMS. There is no specific description of the C&I aspects of the PRMS although its operational performance in both normal and “under degraded” conditions is outlined, which implies that each radiation monitoring system channel are likely to perform safety functions across HPC.

89 The classification of the C&I safety systems and equipment of the PRMS is not specified in sub-chapter 12.3 and there is insufficient detail provided to enable an assessment of their suitability for use at HPC. However, a further description of PRMS and its associated radiation protection instrumentation is described in the sub-chapter 7.6 in terms of a range of Category A safety functions (see 3.1.6 above).

4 ONR ASSESSMENT

90 This assessment has been carried out in accordance with ONR How2 BMS document PI/FWD, “Purpose and Scope of Permissioning” (Ref. 2).

4.1 Scope of Assessment Undertaken

91 I consider that my assessment of PCSR2012 in terms of the scope of C&I safety systems and equipment within the UKEPR™ units has been sufficient for me to reach initial conclusions as to whether NNB GenCo Ltd, as licensee, and its RD has presented adequate information to demonstrate that these are suitable for use at HPC.

92 As previously indicated in this assessment report, it is evident to me that the information for those C&I safety systems within the scope of ONR’s GDA for the UKEPR™ , covered in the main by sub-chapters 7.1 to 7.7, will require further update to align with ONR expectations for the C&I workstream at the end of GDA (Ref. 20). This work will need to be represented in the further work being carried out by NNB GenCo Ltd and its RD, as part of its Basic Design Reference (BDR) exercise.

93 Also, I have found that there is an absence in PCSR2012 of design detail and related information within those sub-chapters that cover C&I safety system and equipment intended for use at HPC which are outside the scope of GDA or the limited additional site specific information in relation to those systems covered in GDA . This matter has been raised with NNB GenCo Ltd by ONR’s C&I workstream at routine Level 4 interactions and is subject of ongoing developments within the RD.

94 On the basis of the above, I consider that PCSR2012 provides insufficient information in terms of the claims, supporting arguments and evidence important to demonstrating the adequacy of the C&I safety systems and equipment for use at HPC. My assessment of a sample of sub-chapters has been made in respect of the claims and arguments to determine if the evidence adequately supports them.

4.2 Assessment

95 My assessment has been made with reference to the SAPs given in Table 1 although due to the limited information provided on some aspects of the C&I systems and equipment it has not been possible to perform a complete assessment in each case. Also, it should be noted that a number of the AFs arising from GDA close-out (Ref. 20) are applicable to address shortfalls in the information provided in PCSR2012 with respect to a number of SAPs.

96 In view of this, my assessment has grouped together SAPs to consider to what extent PCSR2012 can be considered to satisfy those engineering principles important to C&I safety systems and equipment proposed for use within UKEPR™ units at HPC.

4.2.1 Engineering principles: safety classification and standards (ECS.1, ECS.2, ECS.3, ECS.4, ECS.5)

97 It is acknowledged by NNB GenCo Ltd and its RD within PCSR2012 that the C&I safety systems and equipment require categorisation and classification on the basis of potential consequences of faults (including failure to deliver safety functions and postulated initiating faults) that may occur at a UKEPR™. The categorisation and classification within PCSR2012 for C&I safety systems and equipment has been applied to those covered by sub-chapters 7.3 to 7.6 in accordance with an earlier revision of Ref.5. This work claimed to categorise relevant safety functions and classes to systems in a hierarchical manner that aligns with the requirements of BS IEC 61226 (Ref. 21) in terms of their safety significance.

98 NNB GenCo Ltd should confirm that the results of the categorisation and classification studies for those C&I safety systems and equipment covered by sub-chapters 7.3 to 7.6 is not affected by application of methodology given in Ref. 5, which I understand represents the approach agreed in the resolution of a relevant GDA issue on this subject.

99 The approach taken in sub-chapters 7.3 to 7.6 has not been applied within PCSR2012 to other C&I safety systems, such as those associated with the turbo generator sets or MSSS, and NNB GenCo Ltd should apply Ref. 5 to confirm their categorisation and classification before publication of the next revision of HPC PCSR.

100 PCSR2012 in sub-chapter 7.7 makes specific reference to those standards and codes that are to be used as the basis for compliance for the C&I safety systems covered by sub-chapters 7.3 to 7.5. this is an exhaustive listing of relevant international standards, which should ensure that their design, construction, installation and quality assurance are adequately addressed. There is, however, only limited evidence provided for compliance with relevant standards and it is noted that this shortfall was identified during GDA (Ref. 20) through a number of AFs, such as AF-UKEPR-CI-001, AF-UKEPR-CI-006, AF-UKEPR-CI-029, AF-UKEPR-CI-030 and AF-UKEPR-CI-042.

101 In my opinion, there is a need for this same approach to be applied to C&I safety systems outside the scope of GDA.

4.2.2 Engineering principles: equipment qualification (EQU.1)

102 PCSR2012 provides generic statements, with the exception of the platforms, devices and tools covered in sub-chapter 7.7, on the qualification procedures applicable to a number of the C&I safety systems for use within the UKEPR™ units at HPC. This sub-chapter states that the platforms, devices and tools will be subject to a two-legged approach, comprising production excellence activities and ICBMs, to the substantiation of their design in terms of hardware and software.

103 The C&I safety systems and equipment outside the scope of sub-chapter 7.7 (i.e. those safety systems not associated with the nuclear island), should have specific equipment qualification requirements developed so that the NNB GenCo Ltd can demonstrate their safety classification. This matter is likely to be addressed by NNB GenCo Ltd through relevant GDA AFs, such as AF-UKEPR-CI-023, as the design of these C&I safety systems evolves and it is anticipated that these will be elaborated[15] in the next revision of the PCSR for HPC.

104 The equipment qualification requirements can be considered to largely focus on the C&I safety systems and equipment and it is apparent from my assessment of those sub-chapters sampled that little attention appears to have been given to the means of interconnecting the systems, namely cables, wiring and means of termination. This shortfall needs to addressed by NNB GenCo Ltd in sub-chapter 8.4 as these aspects of the C&I safety systems covered in the PCSR may be vulnerable to hazards that may occur in the operational environment at HPC, such as temperature, moisture, humidity, and radiation (Ref. 22).

105 Similarly, I have found that equipment qualification of C&I safety systems and equipment against adverse electromagnetic interference is not adequately covered in the sub-chapters sampled as part of my assessment. This matter is likely to be addressed by NNB GenCo Ltd as the design of the C&I safety systems evolve and the nature of the operational environment at HPC is determined. Therefore, I anticipate that this aspect of equipment qualification will also be elaborated in the next revision of the PCSR for HPC.

4.2.3 Engineering principles: design for reliability (EDR.1, EDR.2, EDR.3, EDR.4)

106 The sub-chapters of PCSR2012 that have been sampled as part of my assessment make reference to various aspects of design for reliability, including single failure criterion, failsafe principles, redundancy, diversity and segregation which align with the requirements of relevant SAPs. However, in my opinion, PCSR2012 does not provide sufficient details of the design of the C&I safety systems for a complete review to be carried out at this time. Nevertheless it is known that those safety systems subject to GDA are to be designed to achieve appropriate levels of redundancy and diversity commensurate with their classification.

107 Nevertheless, I know, from my interactions with NNB GenCo Ltd and its RD at workshops and Level 4 meetings, that the extent of design optimisation necessary to meet the outcomes of GDA has implications for the design of C&I safety systems that have yet to be finalised. The outcome of GDA is likely to involve incorporating additional Category A and B functions within the C&I safety systems that may affect the design and construction

[15] Where this phrase elaborated or similar is used in the section of my report the level of detail is commensurate with that of a PCSR and would cover information on specification of requirements but not on implementation information which would be included in a later safety justification, for example a pre-commissioning safety report.

of equipment cubicles within the equipment rooms proposed for HPC. This matter is currently subject to NNB GenCo Ltd's BDR procedures and ONR oversight to ensure that the GDA outcomes are, so far as is reasonably practicable, fully satisfied. Therefore, I anticipate that measures associated with the design for reliability will be incorporated in the C&I safety systems intended for use at HPC and the implementation of these measures should be more fully elaborated in the next revision of the PCSR for HPC.

108 I have found that those sub-chapters of PCSR2012 sampled as part of my assessment which cover C&I safety systems outside the scope of GDA, namely those associated with the turbo generators, MSSS and PRMS, are also stated to incorporate appropriate measures, such as the single failure criterion, to reflect their assigned classification. However, the absence of detailed information on the design of their C&I safety systems means that there is insufficient evidence at this time to demonstrate the effectiveness of any measures and it is unclear to me to what extent diversity has been considered, for example, as part of those C&I systems and equipment to be used in the MSSS.

109 In my opinion, whilst PCSR2012 clearly indicates that the design of the C&I safety systems will incorporate measures to assure their reliability, the absence of detailed design information supported by relevant analyses (e.g. failure mode, effects and criticality analysis (FMECA)) results in a partial demonstration that these adequately meet the required level of reliability in each case. However, it is anticipated that this information will be available when the detailed designs approach completion and, as such, should be more fully elaborated in the next revision of the PCSR for HPC.

4.2.4 Engineering principles: forms of claims (ERL.1, ERL.2, ERL.3)

110 I have found that PCSR2012 does not contain the results of reliability analyses as required by ERL.1 to verify that C&I safety systems and equipment described in the sub-chapters sampled meet their assigned targets. This appears to result from the incomplete nature of the design of a number of these systems as outlined above and it should be noted that this shortfall was identified during GDA in AF-UKEPR-CI-010 for the PS (see Ref. 20). In my opinion, there is a need for this same approach to be applied to C&I safety systems outside the scope of GDA.

111 The PCSR2012 sub-chapters that I have assessed state that quality assurance (QA) procedures will be used to demonstrate the adequacy of measures used in the design of C&I safety systems and equipment. There are only limited details on the extent of the QA procedures and it is anticipated that this information will be more fully elaborated in the next revision of the PCSR for HPC in order to satisfy ERL.2.

112 I am generally satisfied from PCSR2012 and my Level 4 interactions with NNB GenCo Ltd that the design concepts for the C&I safety systems have taken into account the need for automatically initiated safety features to achieve implementation of protection functions in a timely manner as required by ERL.3. This is reflected in the functional prioritisation rules and architecture of the C&I safety systems described in sub-chapter 7.2 (Ref. 9).

4.2.4 Engineering principles: maintenance, inspection and testing (EMT.1, EMT.3)

113 The PCSR2012 sub-chapters that I have assessed provide an outline of the maintenance and proof testing requirements for each of the C&I safety systems. This work appears to reflect good practice in terms of the classification of any maintenance and test equipment, procedures to be applied and frequency of in-service testing to prove, so far as is reasonably practicable, the complete system. The information provided adequately demonstrates that matters relating to maintenance and in-service testing have been considered by NNB GenCo Ltd and its RD as required by EMT.1.

114 Nevertheless, I have found only limited information on the in-service test equipment. It is anticipated that this will be available when the design(s) are complete and should be more fully elaborated in the next revision of the PCSR for HPC.

115 I am satisfied that the need for type testing as required by EMT.3 has been identified by NNB GenCo Ltd and its RD for those C&I safety systems covered by sub-chapters 7.3 to 7.5 (Refs. 10 to 12) and 7.7 (Ref. 14). However, this aspect has not been addressed for those C&I safety and equipment outside the scope of these sub-chapters and this matter should be addressed in the next revision of the PCSR for HPC.

4.2.5 Engineering principles: external and internal hazards (EHA.10)

116 As stated in 4.2.2 above, I have found that equipment qualification of C&I safety systems and equipment against adverse electromagnetic interference (EMI) is not adequately covered in the sub-chapters sampled as part of my assessment. The measures proposed to be provided at HPC as required by EHA.10 are referred to in sub-chapter 10.3 (Ref. 16) that refers to earthing, which in itself may be insufficient to protect against all forms of EMI. This matter is likely to be addressed by NNB GenCo Ltd as the design of the C&I safety systems evolve and the nature of the operational environment at HPC is determined. Therefore, I anticipate that this aspect of C&I system and equipment protection and any additional measures that may introduced at HPC will be more fully elaborated in the next revision of the PCSR for HPC.

4.2.6 Engineering principles: safety systems (ESS.27)

117 I have found that PCSR2012 sub-chapter 7.7 (Ref. 14) provides an outline of the approach proposed to taken for the design substantiation of the computer-based C&I platforms for Class 1 and 2 systems which aligns with the requirements of ESS.27. The proposed approach describes a combination of production excellence activities and ICBMs which is, as necessary, supported by QA procedures and independent reviews. The extent to which these measures demonstrate that ESS.27 maybe satisfied was addressed by ONR during GDA (Ref. 20) and a number of AFs, such as AF-UKEPR-CI-026, AF-UKEPR-CI-033 and AF-UKEPR-CI-039.

118 The technology of the C&I safety systems and equipment outside the scope of GDA is not specifically described in PCSR2012 and, as such, I am not able to comment on the extent to which their design and substantiation may fulfil the requirements of ESS.27. However, I would expect that a similar approach to that described above be applied in the next revision of the PCSR for HPC.

4.2.7 Engineering principles: control and instrumentation of safety-related systems (ESR.5)

119 PCSR2012 sub-chapter 7.7 (Ref.14) clearly identifies that smart devices not intended for use in nuclear safety applications are to comply with the relevant requirements of BS EN 61508 using the EMPHASIS method[16] to establish production excellence. In my opinion, this approach, which should be supported by relevant compensating measures, is appropriate to demonstrate the requirements of ESR.5 can be satisfied for smart devices and similar equipment that may form part of C&I safety-related systems at HPC.

[16] The EMPHASIS method was developed by the UK's C&I Nuclear Industry Forum (CINIF) and is widely recognised as an appropriate means of determining compliance with BS EN 61508 (Ref. 23) in terms production excellence.

120 It is noted that smart devices intended for use in nuclear safety applications are subject of GDA AF-UKEPR-CI-051 (Ref. 20).

5 CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

121 This report presents the findings of my assessment of those parts of NNB GenCo Ltd's PCSR2012 for HPC that fall within the scope of ONR's C&I workstream and takes into account that this PCSR will be superseded by a further revision which should be a consolidation of the HPC site-specific aspects, the final GDA PCSR and other design changes from FA3.

122 To conclude, my assessment has found that the claims, arguments and evidence laid down within PCSR2012 are at this time insufficient for ONR to support permissioning of the C&I safety systems and equipment intended for use at HPC. This is due to the incomplete nature of the design and development of the new C&I safety systems and equipment required to fulfil the GDA outcomes and providing adequate information on those systems and equipment important to safety that are associated with the balance of plant outside the scope of GDA.

123 I would acknowledge that a number of the shortfalls identified in my assessment report have already been raised with NNB GenCo Ltd and its RD so that they can be addressed as part of the design and development of the C&I safety systems covered in the PCSR. I have also raised a Level 3 Issue an entry on the ONR Issues database (Ref. 24), on those shortfalls that have not been specifically addressed by actions assigned to NNB GenCo Ltd to date. These will also be covered by routine regulatory business.

124 I consider that PCSR2012 should be recorded in the Integrated Intervention Strategy (IIS) database with a rating of 4 (Yellow), below standard. This is in recognition that PCSR2012 is considered to require further work as outlined above.

125 **Level 3 Issue**: In the context of C&I systems important to safety at HPC, NNB GenCo Ltd should ensure that the following are addressed in the next revision of the PCSR:

- compliance with relevant standards for C&I systems and equipment important to safety, such as turbo generator protection systems and C&I systems associated with the main steam system, that are currently outside the scope of existing AFs identified by ONR during GDA. This may be achieved by applying a similar approach that needs to be taken in the resolution of AFs, such as AF-UKEPR-CI-001, AF-UKEPR-CI-006, AF-UKEPR-CI-029, AF-UKEPR-CI-030 and AF-UKEPR-CI-042, to these systems.
- equipment qualification procedures applicable to C&I safety systems and equipment should adequately cover:
  - means of interconnecting systems, namely cables, wiring and points of termination taking into account the operational environment at HPC, such as temperature, moisture, humidity, and radiation, and relevant standards and guidance (e.g. IAEA report NP-T-3.6) on this topic.
  - protective measures to be applied at a system, equipment, component and/or facility level against adverse electromagnetic interference. This should include earthing arrangements and other means necessary to protect against all forms of electromagnetic phenomena that may foreseeably occur at HPC.

- design of C&I safety systems, including those systems covered by GDA which may be modified in order to achieve outcomes agreed with ONR, should be demonstrated to meet their reliability targets through implementing measures to assure their reliability complete with supporting analyses (e.g. failure mode, effects and criticality analysis). This applies in particular to those C&I systems and equipment important to safety, such as turbo generator protection systems and C&I systems associated with the main steam system, that are currently outside the scope of existing AFs on this topic.
- information should be provided on in-service test equipment for use with C&I safety systems and equipment at HPC to demonstrate both its functionality and reliability is commensurate with relevant classification criteria.
- technology selection for C&I safety systems and equipment outside the scope of GDA should be provided complete with details of their design and substantiation to enable an evaluation of compliance with relevant ONR SAPs, such as EDR.1 to 4 on design for reliability and ESS.27 for computer-based systems.

5.2 Recommendations

126 There are no specific recommendations coming from this work reflecting the interim nature of HPC PCSR2012.

6 REFERENCES

1 NNB GenCo Submission of HPC PCSR 2012, Letter NNB-OSL-RIO-000322, ONR-HPC-20337N, 6 December 2012 (TRIM Ref. 2013/16143).

2 *ONR How2 Business Management System. Purpose and Scope of Permissioning.* PI/FWD Issue 3. HSE. August 2011. www.hse.gov.uk/nuclear/operational/assessment/index.htm.

3 *Safety Assessment Principles for Nuclear Facilities.* 2006 Edition Revision 1. HSE. January 2008. www.hse.gov.uk/nuclear/SAP/SAP2006.pdf.

4 *Safety Systems*, T/AST/003 Issue 6.
Electromagnetic Compatibility, NS-TAST-GD-015 Revision 1.
Essential Services, NS-TAST-GD-019 Revision 2.
Computer Based Safety Systems,NS-TAST-GD-046 Revision 3.
www.hse.gov.uk/nuclear/operational/tech_asst_guides/index.htm.

5 *Classification of structures, systems and components,* NEPS-F DC 557 Revision D. AREVA NP, October 2012 (TRIM Ref. 2012/424300).

6 *Safety Assessment Principles for Nuclear Facilities – Subset for NP&E assessment*, 2006 Edition, HSE.

7 *Nuclear Power Plants – Instrumentation and Control Important to Safety – General Requirements for Systems.* BS EN 61513:2013. British Standards Institution (BSI). www.bsigroup.co.uk

8 PCSR –Sub-chapter 7.1 – Design principles of the Instrumentation and Control systems, UKEPR-0002-071 Issue 03 (TRIM Ref. 2013/19255).

9 PCSR – Sub-chapter 7.2 – General architecture of the Instrumentation and Control systems, UKEPR-0002-072 Issue 03 (TRIM Ref. 2012/19276).

10 PCSR – Sub-chapter 7.3 – Class 1 instrumentation and control systems, UKEPR-0002-073 Issue 03 (TRIM Ref. 2013/19282).

11 PCSR – Sub-chapter 7.4 – Class 2 instrumentation and control systems, UKEPR-0002-074 Issue 03 (TRIM Ref. 2013/19288).

12 PCSR – Sub-chapter 7.5 – Class 3 Instrumentation and control systems, UKEPR-0002-711 Issue 00 (TRIM Ref. 2013/19301).

13 PCSR – Sub-chapter 7.6 – Instrumentation, UKEPR-0002-075 Issue 03 (TRIM Ref. 2013/19309).

14 PCSR – Sub-chapter 7.7 – I&C tools, development process and substantiation, UKEPR-0002-076 Issue 03 (TRIM Ref. 2013/19317).

15 NNB Generation Company Ltd, Hinkley Point C Pre Construction Safety Report, Sub Chapter 10.2 Presentation of the Turbogenerator Set, Part of Chapter 10 Steam and power Conversion systems, HPC-NNBOSL-U0-000-RES-000023 Version 1.0 (TRIM Ref. 2013/19571).

16 PCSR – Sub-chapter 10.3 – Main steam system (safety classified part), UKEPR-0002-103 Issue 03 (TRIM Ref. 2013/19582).

17 PCSR – Sub-chapter 12.3 – Radiation protection measures, UKEPR-0002-123 Issue 03 (TRIM Ref. 2013/21023).

18 Design and Construction Rules for Electrical Components of PWR Nuclear Islands. RCC-E. AFCEN. Edition December 2005.

19 *Level 4 – UKEPR I&C Systems for HPC/SZC, 4 December 2013 Teleconference*, NNB GenCo Ltd (TRIM Ref. 2013/460277).

20 *Generic Design Assessment – New Civil Reactor Build, GDA step 4 and Close-out for Control and Instrumentation Assessment of the EDF and AREVA UK EPR™ Reactor, Assessment Report: ONR-GDA-AR-11-022 Revision 1, March 2013,* Office for Nuclear Regulation www.hse.gov.uk/newreactors.

21 *Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions,* BS EN 61226:2010, British Standards Institution (BSI). www.bsigroup.co.uk

22 *Assessing and Managing Cable Ageing in Nuclear Power Plants,* NP-T-3.6 (2012), IAEA Nuclear Energy Series.

23 *Functional Safety of Electrical, Electronic and Programmable Electronic Safety-related Systems, Part 1: General Requirements.* BS EN 61508-1:2010, British Standards Institution (BSI). www.bsigroup.co.uk

24 ONR Regulatory Issue #1907.

Table 1

Relevant Safety Assessment Principles Considered During the Assessment

SAP No.	SAP Title	Description
ECS.1	Engineering principles: safety classification and standards. Safety categorisation	The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be categorised based on their significance with regard to safety.
ECS.2	Engineering principles: safety classification and standards. Safety classification of structures, systems and components.	Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance with regard to safety.
ECS.3	Engineering principles: safety classification and standards. Standards.	Structures, systems and components that are important to safety should be designed, manufactured, constructed, installed commissioned, quality assured, maintained, tested and inspected to the appropriate standards.
ECS.4	Engineering principles: safety classification and standards. Codes and standards.	For structures, systems and components that are important to safety, for which there are no appropriate established codes or standards, an approach derived from existing codes or standards for similar equipment, in applications with similar safety significance, may be applied.
ECS.5	Engineering principles: safety classification and standards. Use of experience, tests or analysis.	In the absence of applicable or relevant codes and standards, the results of experience, tests, analysis, or a combination thereof, should be applied to demonstrate that the item will perform its safety function(s) to a level commensurate with its classification.
EQU.1	Engineering principles: equipment qualification. Qualification procedures.	Qualification procedures should be in place to confirm that structures, systems and components that are important to safety will perform their required safety function(s) throughout their operational lives.

Table 1

Relevant Safety Assessment Principles Considered During the Assessment

SAP No.	SAP Title	Description
EDR.1	Engineering principles: design for reliability. Failure to safety.	Due account should be taken of the need for structures, systems and components important to safety to be designed to be inherently safe or to fail in a safe manner and potential failure modes should be identified, using a formal analysis where appropriate.
EDR.2	Engineering principles: design for reliability. Redundancy, diversity and segregation.	Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components important to safety.
EDR.3	Engineering principles: design for reliability. Common cause failure.	Common cause failure (CCF) should be explicitly addressed where a structure, system or component important to safety employs redundant or diverse components, measurements or actions to provide high reliability.
EDR.4	Engineering principles: design for reliability. Single failure criterion.	During any normally permissible state of plant availability no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function.
ERL.1	Engineering principles: reliability claims. Form of claims.	The reliability claimed for any structure, system or component important to safety should take into account its novelty, the experience relevant to its proposed environment, and the uncertainties in operating and fault conditions, physical data and design methods.
ERL.2	Engineering principles: reliability claims. Measures to achieve reliability.	The measures whereby the claimed reliability of systems and components will be achieved in practice should be stated.
ERL.3	Engineering principles: reliability claims. Engineered safety features.	Where reliable and rapid protective action is required, automatically initiated engineered safety features should be provided.

Table 1

Relevant Safety Assessment Principles Considered During the Assessment

SAP No.	SAP Title	Description
EMT.1	Engineering principles: maintenance, inspection and testing. Identification of requirements.	Safety requirements for in-service testing, inspection and other maintenance procedures and frequencies should be identified in the safety case.
EMT.3	Engineering principles: maintenance, inspection and testing. Type-testing.	Structures, systems and components important to safety should be type tested before they are installed to conditions equal to, at least, the most severe expected in all modes of normal operational service.
EHA.10	Engineering principles: external and internal hazards. Electromagnetic interference.	The design of facility should include protective measures against the effects of electromagnetic interference.
ESS.27	Engineering principles: safety systems. Computer-based safety systems.	Where the system reliability is significantly dependent upon the performance of computer software, the establishment of and compliance with appropriate standards and practices throughout the software development life-cycle should be made commensurate with the level of reliability required, by a demonstration of “production excellence” and “confidence-building” measures.
ESR.5	Engineering principles: control and instrumentation of safety-related systems. Standards for computer based equipment.	Where computers or programmable devices are used in safety-related systems, evidence should be provided that the hardware and software are designed, manufactured and installed to appropriate standards.