Health and Safety Executive

NUCLEAR DIRECTORATE

GENERIC DESIGN ASSESSMENT – NEW CIVIL REACTOR BUILD

STEP 3 CONTROL AND INSTRUMENTATION ASSESSMENT OF THE WESTINGHOUSE AP1000

DIVISION 6 ASSESSMENT REPORT NO. AR 09/037-P

HSE Nuclear Directorate
Redgrave Court
Merton Road
Bootle
Merseyside L20 7HS

EXECUTIVE SUMMARY

This reports presents the findings of the Control and Instrumentation (C&I) assessment of the Westinghouse Electric Company (WEC) AP1000 Pre-Construction Safety Report (PCSR) (Ref. 1) undertaken as part of Step 3 of the Health and Safety Executive's (HSE) Generic Design Assessment (GDA) process.

Scope of Assessment carried out

The report provides an overview of the safety case presented in the PCSR and the standards and criteria adopted in the assessment. The report presents the results of ND's assessment, on a sampling basis, primarily directed at the C&I system level and an initial analysis of the Requesting Party's (RP's) supporting arguments. The assessment was undertaken in accordance with HSE guidance (e.g. Safety Assessment Principles (SAPs) and assessment guides etc.).

WEC's safety arguments are set out in the PCSR. These include compliance to US C&I standards and guidance, and C&I provisions that would be expected of a modern nuclear reactor such as:

- safety systems (e.g. reactor shutdown systems such as the Protection and Safety Monitoring System (PMS) and Diverse Actuation System (DAS);
- plant control and monitoring systems (e.g. the Plant Control System (PLS) that performs functions such as reactor power control);
- main control room with backup via the remote shutdown workstation, and communication systems for information transfer within and external to the plant.

ND's C&I assessment sample covered topics of particular relevance to C&I system level design including review of C&I system architecture, diversity of systems implementing reactor protection functionality and a subset of SAPs considered to be relevant to system level assessment. To assist with the C&I Step 3 assessment a Technical Support Contractor (TSC) was engaged to undertake technical reviews of SAP argumentation, system architecture and diversity. Points requiring clarification and technical review observations were raised by Technical Queries (TQs).

Conclusion

As a result of the Step 3 C&I assessment I conclude that:

a) The PCSR and supporting documentation address the main C&I systems expected in a modern nuclear reactor but the safety case argumentation needs improvement.

b) While the AP1000 C&I architecture is not unacceptable further assessment of the sensitivity of the PMS and DAS reliability figures is necessary and this may lead to the need to review the C&I architecture.

c) Further substantiation is required to support the classification of the DAS, its contribution to the safety groups that implement Category A (reactor protection) functionality and adequacy of the diversity between the DAS and PMS.

d) The DAS design is incomplete and this may lead to aspects of the DAS being subject to GDA exclusion(s). Writing the actual application code for the UK implementation of the PMS is a GDA exclusion (declared out of GDA scope by WEC). The process for development of the application code is within GDA scope.

So far no C&I related Regulatory Issues have been identified and WEC's readiness to address TQs is encouraging. Overall, I see no reason, on C&I grounds, why the WEC AP1000 should not proceed to Step 4 of the GDA process.

LIST OF ABBREVIATIONS

BMS	(Nuclear Directorate) Business Management System
C&I	Control and Instrumentation
CAE	Claims-Argument-Evidence
CCF	Common Cause Failure
CINIF	Control and Instrumentation Nuclear Industry Forum
DAS	Diverse Actuation System
DCD	Design Control Document
FPGA	Field Programmable Gate Array
GDA	Generic Design Assessment
HSE	The Health and Safety Executive
IAEA	The International Atomic Energy Agency
IEEE	Institute of Electrical and Electronics Engineers
NARPS	Next generation Analysis of Reactor Protection Systems
ND	The (HSE) Nuclear Directorate
NRC	Nuclear Regulatory Commission
PCER	Pre-construction Environment Report
PCSR	Pre-construction Safety Report
PIE	Postulated Initiating Event
PLS	Plant Control System
PMS	Protection and Safety Monitoring System
TAG	(Nuclear Directorate) Technical Assessment Guide
TQ	Technical Query
RI	Regulatory Issue
RP	Requesting Party
SAP	Safety Assessment Principle
TSC	Technical Support Contractor
WEC	Westinghouse Electric Company LLC

TABLE OF CONTENTS

1 INTRODUCTION

1 This reports presents the findings of the Control and Instrumentation (C&I) assessment of the Westinghouse Electric Company LLC (WEC) AP1000 Pre-Construction Safety Report (PCSR) (Ref. 1) undertaken as part of Step 3 of the Health and Safety Executive's (HSE) Generic Design Assessment (GDA) process. This assessment has been undertaken in line with the requirements of the Business Management System (BMS) document AST/001 (Ref. 2) and its associated guidance document G/AST/001 (Ref. 3). AST/001 sets down the process of assessment within the Nuclear Directorate (ND) and explains the process associated with sampling of safety case documentation. The Safety Assessment Principles (SAPs) (Ref. 4) have been used as the basis for the assessment of the C&I associated with the AP1000 design. Ultimately, the goal of assessment is to reach an independent and informed judgment on the adequacy of a nuclear safety case.

2 The report provides an overview of the safety case presented in the PCSR and the standards and criteria adopted in the assessment. The report presents the results of ND's C&I system level assessment and initial analysis of the Requesting Party's (RP) supporting arguments. NB. An "argument" is defined as "the set of evidence components that support a claim, together with a specification of the relationship between these evidence components and the claim" (Ref. 5).

3 The assessment was undertaken in accordance with the Step 3 C&I Project Initiation Document (PID) (Ref. 6) and HSE guidance (e.g. on a sampling basis). Points requiring clarification and technical review observations have been raised by Technical Queries (TQs) (Ref. 7). Points of significant safety concern are covered by Regulatory Issues (RI). No RIs were raised during our Step 3 assessment of the AP1000 C&I.

2 NUCLEAR DIRECTORATE'S ASSESSMENT

2.1 Requesting Party's Safety Case

4 WEC provided a number of documents setting out its C&I safety case and a submission outlining where the SAPs are addressed in the documents. The main submission that describes the C&I is the Design Control Document (DCD) Ref. 8. The C&I provisions claimed include those that would be expected of a modern nuclear reactor such as:

- safety systems (e.g. reactor shutdown systems such as the Protection and Safety Monitoring System (PMS) and Diverse Actuation System (DAS);
- plant control and monitoring systems (e.g. the Plant Control System (PLS) that performs functions such as reactor power control);
- main control room with backup via the remote shutdown workstation;
- communication systems for information transfer within and external to the plant.

5 The WEC submissions on C&I mainly describe a conceptual design and WEC explains that the "design certification" of the AP1000 focuses on the process used to design and implement the C&I rather than on the specific implementation. WEC also explain that the description of the PMS is based on the Common Q platform and it is noted that this platform has been generically approved by the United States (US) Nuclear Regulatory Commission (NRC). The DAS is to be based on Field Programmable Gate Array (FPGA) technology using a process approved by the US NRC for a non-reactor protection application.

6 An important aspect of the safety demonstration is the classification of systems important to safety and the application of appropriate design standards. The accepted practice is that the standards are more onerous for those systems that are more important to safety. In the UK the importance to safety is typically judged by a combination of deterministic

(e.g. the function performed by the system such as to shut down the reactor) and probabilistic (the reliability required of the system) criteria. The WEC AP1000 C&I design concept reflects US custom and practice, and is largely based on US C&I standards (e.g. Institute of Electrical and Electronics Engineers (IEEE) standards) and US NRC requirements. Two system classifications are used (i.e. safety-related and non-safety related).

2.2 Standards and Criteria

7 The standards and criteria used for the C&I Step 3 assessment include:

- a subset of SAPs considered to be relevant at the system level (Table 1);
- relevant sections of HSE Technical Assessment Guides (TAGs) (e.g. Ref. 9 and Ref. 10) and regulatory guidance (Ref. 5);
- relevant nuclear sector standards related to C&I system level design, system architecture and diversity of systems (e.g. Ref. 11 and 12 etc.).

2.3 Nuclear Directorate Assessment

8 During Step 3 the RP's safety case argumentation was assessed using a subset of SAPs considered to be relevant at the C&I system level (Table 1). Aspects of particular relevance to C&I system level design were also assessed, namely:

- C&I system architecture;
- diversity of systems implementing reactor protection functionality.

9 To assist with the C&I Step 3 assessment a Technical Support Contractor (TSC) was engaged to undertake technical reviews of SAP argumentation, system architecture and diversity. The TSC's reports (Refs 13, 14 and 15) provide the technical opinion of the TSC. I specified and undertook reviews of the TSC's work. Following review, all areas requiring further clarification were raised with the RP by TQ. Assessment of the RP's TQ responses will continue during Step 4.

2.3.1 Step 3 SAP Assessment

10 A list of the SAPs used to assess the adequacy of the RP's safety case argumentation during Step 3 can be found in Table 1. In selecting the SAPs for Step 3 particular attention was given to those SAPs considered to have particular relevance to system and architectural design. A detailed report on the adequacy of the RP's safety case argumentation was produced by the TSC (Ref. 13). Annex 2 contains a table of the TSC's main findings and observations. As a result of the SAP argumentation assessment it is concluded that:

- While WEC claim compliance to the SAPs, further argumentation and evidence will need to be provided to substantiate the claims.
- The SAP Roadmap provided by WEC (Ref. 16) does not readily identify all the relevant information within the DCD or PCSR and contains some information that should be in the safety case.
- The DCD and the PCSR do not always reference the available evidence that supports the claims (e.g. references to the W-CAP documentation supplied).
- The C&I design is not yet complete (e.g. DAS) and this has limited the depth of assessment.

- The WEC safety case Claims-Arguments-Evidence (CAE) diagrams supplied in support of the PCSR (Ref. 19) require further development to identify detailed evidence in addition to that already referenced in the PCSR / DCD.
- Safety Categorisation and Classification - The AP1000 two levels of categorisation and classification (i.e. Safety Related and non-Safety Related) do not align with HSE's SAPs (Ref. 4) or BS IEC 61226:2005 (Ref. 17).
- Standards – Further clarification is required in relation to the standards used by WEC and their alignment to nuclear sector international standards.
- Defence-in-Depth – Further clarification is required in relation to the allocation of safety functions to C&I systems (i.e. alignment to the 5 levels of defence-in-depth referred to in International Atomic Energy Agency (IAEA) Safety Standard NS-R-1 (Ref. 18)). However, use is made of two digital platforms (i.e. ABB AC160 and Ovation) and a FPGA based system. The PMS uses the ABB AC160 platform, the PLS is based on the Ovation platform and the DAS is to be implemented using an FPGA.
- Diversity - Equipment diversity is used across the two digital platforms PMS (ABB AC 160) and PLS (Ovation), and the DAS (FPGA based). Further clarification is required on the extent of functional diversity.
- Failure to Safety – Further clarification is required on the fail-safe principle as applied to C&I systems.
- Computer Based Systems Important to Safety – Further clarification is required as to how the independent 'confidence-building' and production excellence legs (Ref. 10) are addressed.

11 The majority of SAP assessments resulted in TQs being raised. The responses to the TQs will continue to be assessed during Step 4.

12 Since the DAS design is incomplete this may lead to aspects of the DAS being subject to GDA exclusion(s). Note that writing the application code for the UK implementation of the PMS is a GDA exclusion (declared out of GDA scope by WEC). The process for development of the PMS application code is within GDA scope.

13 The TSC noted, as one of its main concerns, that the argument for the DAS system not being safety-related requires further clarification given the significant safety-related functions (Category A) such as reactor protection that it performs. WEC has stated (Ref. 19) that the functions the DAS implements are Category A in alignment with the Final Draft International Standard IEC 61226 Edition 3 (now published as IEC 61226:2009). WEC also stated that "the PMS provides the principle means of fulfilling the function, and the DAS provides a significant contribution to fulfilling the function. Therefore, the DAS is implemented in a Class 2 system". This may not be unacceptable provided the DAS reliability target is confirmed to be no better than 1×10^{-2} pfd and the safety groups (of which the DAS is a part) implementing the Category A functions are shown to be adequate (see below).

14 WEC has explained that additional confidence building activities will be undertaken for the PMS including additional independent reviews and statistical testing in support of the system's reliability claim. WEC is working with Bristol University to develop a practical approach to statistical testing.

15 Overall, as a result of the SAP argumentation assessment it is concluded that there is currently insufficient CAE structure in the PCSR to clearly demonstrate how the C&I SAPs are addressed.

2.3.2 C&I System Level Architecture

16 At the start of Step 3 an initial assessment of the AP 1000 C&I architecture was undertaken. The assessment did not reveal any major concerns that would necessitate the raising of a regulatory issue. One area of concern that was identified was the reliability claims on the PMS and PLS (see below).

17 The TSC produced a detailed report on the AP1000 C&I architecture (Ref. 14). Annex 3 contains an overview of the TSC's main findings and observations. The main objective of the work was to consider the overall system architecture (C&I systems) looking at safety design features in the WEC AP1000 submission, namely:

- Defence-in-depth and failure mode management including Common Cause Failure (CCF).
- Independence and diversity.
- Provision for automatic and manual safety actuation.
- Appropriateness of equipment type / class.

18 The TSC work involved defining a list of reactor-independent essential / desirable system architecture characteristics needed to comply with relevant standards and guidance. In selecting the characteristics consideration was given to HSE SAPs (Ref. 4), technical assessment guides (Ref. 9 and 10) and nuclear sector C&I standards (i.e. Ref. 11, 12 and 20).

19 The TSC concluded that the AP1000 C&I architecture is in accordance with many of the relevant nuclear sector principles, standards and guidance documents. However, the TSC identified areas where further clarification and substantiation are required (see Annex 3), the more significant of which include:

- overall specification of the C&I architecture design including the interface requirements between different systems;
- reliability claims for the C&I systems (PMS, DAS and PLS);
- categorisation and classification of systems (in particular DAS categorisation);
- analysis of the adequacy of safety groups (e.g. addressing coverage of Postulated Initiating Events (PIEs), reliability, CCF and single failures etc.);
- DAS FPGA design (including alignment with HSE ND's special case procedure for complex hardware);
- interconnectivity of systems on and off site;
- segregation of C&I systems to ensure a lower class system cannot frustrate the correct operation of a higher class system;
- classification and provision of turbine control and safety display systems.

20 It is important that the C&I architecture is based on an overall consideration of the safety functions that need to be performed including the category and reliability of the functions. In assigning the functions to systems, consideration needs to be given to the maintenance of independence (so that a failure in a lower safety class system does not frustrate the correct operation of systems of a higher safety class) and communication of information to other systems (e.g. communication of important safety display information to the main control room). The rigourous definition of the overall system architecture including assignment of functions to systems and definition of interface requirements assists with the demonstration that there are no safety deficiencies in the overall system architecture.

21 The reliability claims for key C&I systems challenge the accepted claim limits for C&I systems (PMS 1×10^{-5} probability of failure on demand (pfd) and PLS 1×10^{-5} probability of dangerous failure per year (pdfy)). WEC has undertaken a sensitivity study (Ref. 21) to investigate the impact on plant risk of using more modest reliability claims for the C&I systems. WEC's view is that the sensitivity study demonstrates that the plant risk is not unacceptable with more modest reliability claims (e.g. PMS 1×10^{-3} pfd). ND is undertaking an independent review of the sensitivity of the WEC AP1000 Probabilistic Risk Assessment to variations in the reliability claims for the AP1000 C&I systems and this may reveal the need to review the C&I architecture.

22 WEC has explained that its submissions (e.g. PCSR and DCD) are based on the categorisation and classification approach used in the US (Ref. 19) and that the categorisation can be mapped into the approach defined by the IAEA, SAPs and nuclear sector standards (Ref. 17). WEC state that the categorisation will be completed in accordance with its Quality Assurance Procedures as the design is "finalised". WEC has provided a summary of its methodology including a provisional definition of AP1000 C&I functions based on IEC 61226 (Ref. 17) categories and system class in accordance with IEC 61513 (Ref. 11). While the table provided in Attachment 1 of Ref. 19 shows reasonable alignment with our expectations for function category and C&I system class there are a number of areas where we are seeking further clarification (e.g. DAS class dependent on results of ND's reliability assessment (see above), scope of Class 1 displays and manual controls, and Turbine Control system class). Other areas requiring clarification may emerge as a result of the Step 4 assessment.

23 The Step 3 assessment identified the need for WEC to clarify what has been done to analyse the adequacy of safety groups that implement Category A functionality (e.g. reactor protection involving the PMS and DAS). Factors that need to be considered include the coverage of PIEs, reliability required of the safety group (including contribution from the PMS and DAS), the potential for CCFs and single failures etc.

24 The absence of detailed design information (in particular for the DAS) has limited the depth of the assessment (e.g. DAS fail-safe behaviour) and this may result in the need for GDA exclusions. The protection functionality of the DAS is to be implemented in FPGA technology. We consider that an FPGA is complex hardware technology and that the application development process has much in common with traditional software development. As a result we will base our assessment on the SAPs special case procedure for complex hardware and Ref. 10. We will also review the results of the US NRC's safety evaluation of an FPGA based system implemented in a US plant (see below).

25 The interconnectivity of systems on and off site has been reviewed. WEC is to undertake an assessment of computer security using appropriate standards during Step 4 (Ref. 19). The AP1000 design makes use of a Component Interface Module (CIM) to resolve demands for component actuation from devices of different safety class (e.g. PMS and PLS). Note that the UK EPR has a similar arrangement (the Priority and Actuation Control System). Further clarification is being sought as to the adequacy of this arrangement, in particular, that the PLS cannot frustrate correct operation of the PMS (e.g. actuations when demanded). The segregation (physical separation) of C&I systems to ensure a lower class system cannot frustrate the correct operation of a higher class system also requires further demonstration.

26 WEC is to qualify the Safety/Qualified Data Processing System (QDPS) display system internal communications bus (currently the AF100 bus) to Class 1 standards and when the qualification is complete it will be applicable to the AP1000. This will facilitate the provision of safety Class 1 displays and controls to the operator.

27 In conclusion, the C&I architecture includes the main C&I systems and provisions that would be expected in a modern nuclear reactor. While the AP1000 C&I architecture is

not unacceptable further assessment will be required during Step 4. In particular, to review the sensitivity of the PMS, PLS and DAS reliability figures and this may lead to the need to review the C&I architecture. Additionally, further clarification is required in relation to DAS class and its contribution to the safety groups that implement Category A (e.g. reactor protection) functionality.

2.3.3 Diversity of Systems Implementing Reactor Protection Functionality

28 A review of the diversity of those systems implementing reactor protection functionality was undertaken. The C&I safety systems included in the diversity review were the PMS and DAS. These systems were selected because they perform the AP1000 protection functions.

29 The TSC produced a report on the diversity of the PMS and DAS (Ref. 15). Annex 5 contains a table of the TSC's main findings and observations. The approach adopted by the TSC included consideration of various forms of diversity, including:

- Functional and equipment diversity (including diversity of platform).
- Diversity of Verification and Validation.
- Diversity of physical location (segregation).
- Software diversity.
- Data diversity / signal diversity.
- Diversity of design / development.
- Diversity of specification.

30 The work required the definition of a list of reactor-independent diversity characteristics, derived from relevant standards and guidance. In selecting the characteristics, consideration was given to SAP's, technical assessment guides, nuclear sector C&I standards (i.e. Ref. 11 and 12), regulatory guidance (Ref. 5) and relevant research (Ref. 22).

31 In summary, the TSC's report (Ref. 15) on the diversity of systems implementing reactor protection functionality concludes that WEC appears to claim full diversity between the PMS and DAS, but the DAS design is not complete enough to support a full diversity analysis. The documentation does not provide sufficient depth in areas such as diversity argumentation and evidence, analysis of common cause failures between PMS and DAS, analysis of the diversity within the safety groups providing the Category A functionality (including the contribution of the PMS and DAS to the safety groups), coverage of functional and equipment diversity, independence and segregation, maintenance and test, and use of diverse verification and validation.

32 In conclusion, further detailed substantiation is required to demonstrate the adequacy of the diversity between the systems implementing reactor protection functionality (i.e. the DAS and PMS). In completing the detailed demonstration that the PMS and DAS are adequately diverse the RP will need to address the guidance of Appendix 4 of Ref. 10.

2.3.4 Step 2 Observations

33 Regular progress meetings have been held with the RP to progress close out of ND's Step 2 assessment observations (Ref. 23). The RP has produced an action tracking matrix to capture the work required to close out the observations. So far reasonable progress has been made in closing out the observations and the work will extend into Step 4 which, given the progress made, is not considered unreasonable. In carrying out

its work the TSC has included consideration of the Step 2 observations and responses received from the RP.

2.3.5 Use of Overseas Regulators Information

34 The US NRC has completed safety evaluations of the Common Q platform and an application (i.e. Wolf Creek Generating Station – Modification to the main steam and feedwater isolation system control) using the same FPGA technology as that proposed for the AP1000 DAS application. These safety evaluation reports will be considered during our Step 4 assessment.

2.3.6 GDA Related C&I Research

35 Research into the means of justifying graphical based auto-code generators (as used for the implementation of systems based on the ABB AC160 platform) is being undertaken as part of the nuclear industry Control and Instrumentation Nuclear Industry Forum (CINIF) Next generation Analysis of Reactor Protection Systems (NARPS) project. The results of the research, where considered appropriate, will be used to inform ND's assessment.

3 CONCLUSIONS AND RECOMMENDATIONS

36 As a result of the Step 3 C&I assessment I conclude that:

- The PCSR and supporting documentation address the main C&I systems and provisions that would be expected in a modern nuclear reactor but the safety case argumentation and identification of evidence needs improvement.
- While the AP1000 C&I architecture is not unacceptable further assessment of the sensitivity of the PMS and DAS reliability figures is necessary and this may lead to the need to review the C&I architecture.
- Further substantiation is required to support the classification of the DAS, its contribution to the safety groups that implement Category A (reactor protection) functionality and adequacy of the diversity between the DAS and PMS.
- The DAS design is incomplete and this may lead to aspects of the DAS being subject to GDA exclusion(s). Development of the application code for the UK implementation of the PMS is a GDA exclusion (declared out of GDA scope by WEC). The process for development of the application code is within GDA scope.

37 So far no C&I related Regulatory Issues have been identified and WEC's readiness to address TQs is encouraging. Overall, I see no reason, on C&I grounds, why the WEC AP1000 should not proceed to Step 4 of the GDA process.

4 REFERENCES

1 *AP1000 Pre-construction Safety Report.* UKP-GW-GL-732, Revision 1, Westinghouse Electric Company LLC, March 2009.

2 *ND BMS, Assessment Process.* AST/001, Issue 2, HSE, February 2003.

3 *ND BMS, Guide: Assessment Process.* G/AST/001, Issue 2, HSE, February 2003.

4 *Safety Assessment Principles for Nuclear Facilities.* 2006 Edition, Revision 1, HSE, January 2008.

5 *Seven Party task force on safety critical software report on "Licensing of safety critical software for nuclear reactors. Common position of seven European nuclear regulators and authorized technical support organizations"*. Available via the HSE website.

6 *New Reactor Build. Step 3 C&I Assessment Strategy.* ND Division 6 AR 08/018. TRIM Ref. 2008/164681.

7 *Westinghouse AP1000 - Schedule of Technical Queries Raised during Step 3.* HSE-ND, TRIM Ref. 2009/358248.

8 *AP1000 European Design Control Document.* EPS-GW-GL-700, Revision 0, Westinghouse Electric Company LLC,16 February 2009.

9 *ND BMS, Technical Assessment Guide* T/AST/003. Safety Systems, Issue 4, HSE, 10 June 2009.

10 *ND BMS, Technical Assessment Guide* T/AST/046. Computer Based Safety Systems, Issue 2, HSE, 16 June 2008.

11 *BS IEC 61513:2001 Nuclear power plants - Instrumentation and control for systems important to safety – General requirements for systems.* International Electrotechnical Commission (IEC), 2001.

12 *BS IEC 62340:2007 Nuclear power plants - Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF).* International Electrotechnical Commission (IEC), 2007.

13 *NII GDA Technical Review – C&I SAP Compliance Assessment for AP1000* - S.P1440.41.60, Issue 1.1.

14 *NII GDA Technical Review – C&I System Architecture Functional Safety Review Report for Westinghouse AP1000* – 36331/35796R, Issue 1.4.

15 *NII GDA Technical Review – C&I Diversity Aspects of C&I Category A Functional Systems Design Assessment for AP1000* – 36331 / 35867R, Issue 1.7.

16 *Safety Assessment Principles Roadmap for AP1000 Design.* UKP-GW-GL-710, Section C, Revision 2, Westinghouse Electric Company LLC, 28 July 2008.

17 *BS IEC 61226:2005 Nuclear power plants - Instrumentation and control systems important to safety – Classification of instrumentation and control functions.* International Electrotechnical Commission (IEC), 2005.

18 *Safety of Nuclear Power Plants: Design – Requirements.* IAEA Safety Standards Series No. NS-R-1 International Atomic Energy Agency (IAEA) Vienna 2000.

19 *Westinghouse Letter - C&I Step 3.* Westinghouse Electric Company LLC, UN REG WEC 00087, 28 August 2009. TRIM Ref. 2009/343656.

20 *BS IEC 60987:2007 Nuclear power plants - Instrumentation and control important to safety – Hardware design requirements for computer-based systems.*21 *Control and Instrumentation Sensitivity Cases.* UKP-GW-GL-744, Revision 0, Westinghouse Electric Company LLC, 17 December 2008.

22 *Guidance on means to achieve system diversity: DISPO6 view*, Littlewood B, Popov P, Strigini L, Version V1.0 PP_DISPO6_01, 27th October 2008.

23 *New Reactor Build. Westinghouse Step 2 C&I Assessment.* HSE-ND, March 2008. TRIM Ref. 2008/135347.

Table 1

Control & Instrumentation SAPs Considered During Step 3 Assessment

SAP No.	Assessment topic / SAP title
EKP - Key Principles	
EKP.3*	Defence-in-depth
EKP.5*	Safety Measures
ECS - Safety classification and standards	
ECS.1	Safety categorisation
ECS.2	Safety classification of structures, systems and components
ECS.3	Standards
EQU - Equipment Qualification	
EQU.1*	Qualification procedures
ERL - Reliability Claims	
ERL.2*	Measures to achieve reliability
ERL.4*	Margins of Conservatism
EMT - Maintenance, inspection and testing	
EMT.1*	Identification of requirements
EMT.3*	Type testing
EMT.6*	Reliability claims
EMT.7	Functional testing
ELO -Layout	
ELO.1*	Access
EHA - External and internal hazards	
EHA.10*	Electromagnetic interference
EDR, ESS - Failure to safety	
EDR.1	Failure to safety
ESS.21(part)	Reliability – failsafe approach
EKP, EDR, ESS, ERC - Defence-in-depth	
EKP.3*	Defence-in-depth
EDR.2	Redundancy, diversity and segregation
ESS.2(part)	Determination of safety system requirements – Defence-in-depth
ESS.7	Diversity in the detection of fault sequences

SAP No.	Assessment topic / SAP title
ESS.18	Failure independence
ERC.2	Shutdown systems
EDR.3	Common cause failure
EDR.4	Single failure criterion
EKP, ESS, ERL - Safety systems	
EKP.5*	Safety Measures
ESS.1	Requirement for safety systems
ESS.2(part)	Determination of safety system requirements
ESS.3	Monitoring of plant safety
ESS.8	Automatic initiation
ERL.3	Engineered safety features (Automatic initiation)
ESS.9*	Time for human intervention
ESS.10*	Definition of capability
ESS.11*	Demonstration of adequacy
ESS.12*	Prevention of service infringement
ESS.15*	Alteration of configuration, operational logic or associated data
ESS.16*	No dependency on external sources of energy
ESS.19*	Dedication to a single task
ESS.20*	Avoidance of connections to other systems
ESS.21(part)	Reliability – Avoidance of complexity
ESS.23	Allowance for unavailability of equipment
ESS.24*	Minimum operational equipment requirements
ESS, ESR - Computer-based systems important to safety	
ESS.27	Computer-based safety systems
ESR.5	Standards for computer based equipment
ESR - Control and instrumentation of safety-related systems	
ESR.1	Provision in control rooms and other locations
ESR.3	Provision of controls
ESR.4*	Minimum operational equipment
ESR.7	Communications systems
EES - Essential services	
EES.1*	Provision
EES.2*	Sources external to the site
EES.8*	Sources external to the site – only source
EES.9*	Loss of service

SAP No.	Assessment topic / SAP title
EHF - Human Factors	
EHF.7*	User interfaces

SAPs identified with an asterisk e.g. EES.1* are new for Step 3 (i.e. they were not considered during Step 2).

Annex 1 – Control and Instrumentation – Status of Regulatory Issues and Observations

RI / RO Identifier	Date Raised	Title	Status	Required timescale (GDA Step 4 / Phase 2)
Regulatory Issues				
None.				
Regulatory Observations				
None.				

Annex 2 – SAP Argumentation Review - TSC's Main Findings and SAP Summary Review

This annex reproduces below the main findings from the TSC report "NII GDA Technical Review – C&I SAP Compliance Assessment for AP1000 - S.P1440.41.60, Issue 1.1", Ref. 13 and presents a summary of the SAP review extracted from Ref. 13.

Main findings

"*The main findings are as follow:*

AP1000.T3.1 The SAP Compliance Roadmap [9] is not precise enough to enable easy access to all the relevant information within the DCD [10] or PCSR [11].

AP1000 T3.2 The SAP Compliance Roadmap [9] also contains information that should be in the PCSR (for example: the set point modification process).

AP1000 T3.3 The DCD [10] and the PCSR [11] content does not always reference the additional available evidence that supports the claims (for example: references to the W-CAP documentation supplied).

AP1000 T3.4 The argument for the DAS system not being safety-related is not understood in the context of the apparently significant safety-related functions it supplies.

AP1000 T3.5 Westinghouse's response to Technical Queries (TQs) indicates that the C&I design is not yet complete and therefore the depth of assessment in this phase has been limited by the available information.

AP1000 T3.6 The safety case CAE diagrams supplied by Westinghouse to support the PCSR are at too high a level to add much value to the current safety case. More detailed diagrams are required."

Table A2.1 - Summary SAP Review

Note text shown in italics below is reproduced from Ref. 13.

SAP No.	Main Findings / Observations	TQ Summary
ECS - Safety Categorisation, Classification and Standards		
ECS.1	*There is some information within the DCD that indicates that some of the issues required to be addressed by SAP ECS.1 are included. However, this is incomplete and the argument or explanation how this information satisfies all aspects of SAP ECS.1 is weak or not made.*	*The design concept of the AP1000 C&I reflects US custom and practice, and is largely based on US C&I standards and NRC regulatory requirements. As a result the observations largely reflect the difference between US and UK approaches.*
ECS.2	*There is some information relevant to ECS.2 made in response to ECS.1. However, this is incomplete and the argument or justification how AP1000 C&I design satisfies all aspects of SAP ECS.2 requirements has not been made.*	*The compliance response for ECS.2 was included in ECS.1.* *Additional information is required to demonstrate compliance with all requirements related to ECS.2 sub-claims.*
ECS.3	*It is not evident that all systems in the non-safety related category would meet UK classification requirements.*	*The design concept of the AP1000 C&I reflects US custom and practice, and is largely based on US C&I standards.* *Additional information is required to demonstrate compliance with UK requirements for safety related and non-safety related C&I systems.*
EKP, EDR, ESS, ERC - Defence-in-depth		
EKP.3	*The AP1000 roadmap does not argue satisfactorily that the AP1000 meets the SAPs.*	*- The response is incomplete for SAP EKP.3 and not all requirements have been addressed.* *- The response is based on US standards and provides inadequate compliance with UK international and C&I nuclear standards.*
EDR.2	*Only the PMS appears to have been addressed. The DCD/PCSR does not provide clear evidence that:* *1. All sources of CCF have been identified* *2. Impact of CCFs have been analysed* *3. Defences against CCFs have been implemented or risk of CCFs is argued to be acceptable*	*More argumentation and information is required to demonstrate compliance with this SAP.*
EDR.3	*There is no overall argument that demonstrates that: a rigorous process has been performed to identify the requirements for redundancy, diversity, segregation and reliability within the C&I system and those requirements have been satisfied*	*More argumentation and information is required to demonstrate compliance with this SAP.*
EDR.4	*Evidence to support the claim for the reactor trip system is available. There is no information for the rest of the C&I system.*	*More argumentation and information for the rest of the C&I system is required to demonstrate compliance with this SAP.*

SAP No.	Main Findings / Observations	TQ Summary
ESS.18	*There is not sufficient information provided in the PCSR/DCD to determine that no internal or external fault can disable the safety systems. In addition the segregation of the PMS and DAS systems has not been addressed.*	*Westinghouse could consider making the compliance against specific sections of chapter 3, for example against Appendix 3D. Specifically the requirements for, "No faults in associated systems can disable the safety system" and, "Safety systems should be physically separate, independent, isolated from other systems" do not appear to have been addressed.*
ERC.2	*The reactor protection system PMS and DAS appear to be missing from the description of the reactor shut down system. The C&I elements of the rod control and Boration system need clarifying*	*The assessor would have expected to see the reactor protection systems included in the compliance with this SAP. Westinghouse to explain how compliance with this SAP is achieved and how the reactor protection systems relate to the other reactor shutdown systems.*
ERL, EMT - Reliability Claims / Maintenance, Inspection and Testing		
ERL.2	*1. There is a lack of discussion on the identification and management of systematic errors* *2. There is a lack of detail on the tools and techniques to be used in the reliability analysis* *3. There is a lack of detail on the calculation and use of repair time data for the reliability analysis.*	*Information is requested on 1. Management of components, 2. Tools & techniques, 3. Calculation and use of repair times and 4.Systematic error management.*
ERL.4	*1. There is a lack of detail on the credit that is claimed for multiple safety related systems.* *2. There is a lack of detail about how testing during operations maintenance is applied to each C&I system.*	*Information is requested on management of common cause failures and procedures and equipment for operational testing and maintenance of safety related systems.*
EMT.1	*Of the 3 sub-claims, there is not enough evidence to claim that any are satisfied.*	*More argumentation and information is required to demonstrate compliance with this SAP.*
EMT.3	*Of the 4 sub-claims, there is not enough evidence to claim that 3 are satisfied.*	*More argumentation and information is required to demonstrate compliance with this SAP.*
EMT.6	*There is a lack of information on and argument for the proposed maintenance processes and schedules for safety and safety-related C&I and the related test equipment.* *Component lifetimes for components that wear out need to be included in maintenance schedules to ensure they are replaced before failure.*	*Information is requested on maintenance schedules and how component replacement and testing approaches are justified.*
EMT.7	*There is insufficient argumentation and evidence to demonstrate that all sub-claims have been fully satisfied for all C&I sub-systems.*	*Some information has been found in the DCD to support some of the sub -claims for EMT.7. There is insufficient evidence to demonstrate that all C&I sub-systems have been addressed.*

SAP No.	Main Findings / Observations	TQ Summary
EDR, ESS - Failure to Safety		
EDR.1	*There is insufficient information with the DCD and PCSR to determine if the C&I safety systems are fail safe. In particular it is not clear that the two out of two architecture of the DAS is fail safe.*	*More argumentation and information is required to demonstrate compliance with this SAP.*
ESS.21	*1 Question DAS safety classification as non-safety related;* *2 No justification of complexity levels;* *3 Not enough clarity on the implementation of a failsafe solution;* *4 Not enough justification of fault identification and test processes.*	*More information is requested on justification of actual complexity levels, failsafe solutions and fault identification processes.*
EKP, ESS, ERL - Safety Systems		
EKP.5	*The AP1000 roadmap does not argue satisfactorily that the AP1000 meets the SAPs.*	*- The response is incomplete for SAP EKP.5 and not all requirements have been addressed.* *- The response is based on US standards and provides inadequate compliance with UK international and C&I nuclear standards.* *- The retrace within the DCD is too wide to show compliance against the SAP.*
ESS.1	*It was not possible to identify if the fault sequence initiating events have been adequately terminated, as there is no fault schedule within the documents provided. In addition there is insufficient argumentation that the safety systems are adequate and to demonstrate that risks have been reduced to ALARP.*	*More argumentation and information is required to demonstrate compliance with this SAP for the reduction of risk to ALARP and how the safety systems maintain the system in the shutdown condition, and to describe what fault sequences are mitigated by the various safety features.*
ESS.2	*The information presented here is too general to enable the assessor to determine if the referenced DCD sections provided arguments to show compliance with SAP ESS.2.*	*Westinghouse should provided specific references that point to detailed information within the AP1000 documentation that presents arguments that show how SAP ESS.2 is satisfied. Evidence of compliance to standards relevant to SAP ESS.2 should be provided.*
ESS.3	*(1) The references to DCD chapter 7 sections 7.5.2, 3 and 5 and DCD chapter 18 section 18.8.2 do not lead the assessor to specific detailed arguments that show that SAP ESS.3 has been satisfied.* *(2) The references to DCD information provided within the AP1000 Road Map do not lead the assessor to specific arguments that show how the sub claim P338 is satisfied.*	*Westinghouse shall provided specific references that point to detailed information within the AP1000 documentation that presents arguments that show how SAP ESS.3 and sub claim P338 is satisfied. The assessor would expect the arguments to show that the controls provided are adequate to allow monitoring of the plant state in relation to safety.*

SAP No.	Main Findings / Observations	TQ Summary
ESS.7	*These claims have been reviewed during the Step 2 assessment. The four observations arising remain open and the information requested is relevant to this Step 3 assessment. Therefore this Step 3 assessment requires that information before it can be completed. In addition, for the purposes of this Step 3 assessment the assessor is looking for arguments with supporting evidence that the requirements of SAP ESS.7 have been satisfied.*	*The information provided by the Roadmap and DCD section 7.7.1 does not provide arguments that show that the requirements of SAP ESS.7 have been met in terms of providing evidence in the form of design and implementation documentation, and the compliance to appropriate standards.*
ESS.8	*It is not clear that facility personnel cannot negate the correct safety system action.*	*More argumentation and information is required to demonstrate compliance with this SAP.*
ESS.9	*Of the 2 sub-claims, there is not enough evidence to claim that either is satisfied.*	*More argumentation and information is required to demonstrate compliance with this SAP.*
ESS.10	*Of the 3 sub-claims, there is not enough evidence to claim that any are satisfied.*	*More argumentation and information is required to demonstrate compliance with this SAP.*
ESS.11	*·No fault schedule has been provided. It is not explicitly clear what risks are mitigated by the various safety features, and ·that these are adequate*	*More argumentation and information is required to demonstrate compliance with this SAP.*
ESS.12	*It is not clear how that information contained in the DCD chapters demonstrates that the sub-claims have been addressed.*	*There is information to indicate that the SAP has been addressed, however, the chapters referenced in the Roadmap include a lot of detailed information and it is not clear how that information demonstrates that the sub-claims have been addressed.*
ESS.15	*Application software changes do not appear to have been addressed in either the DCD or PCSR.*	*Information is requested on where the safety analysis that supports changes to the application software system is addressed within the safety case*
ESS.16	*SAP ESS.16 is satisfactorily argued within the Roadmap UKP-GW-GL-710 and evidence of compliance can be found in the DCD Section 7.1.2.13 and* 8.1.4.2.1	*N/A*
ESS.19	*ESS.19 requires a safety system should be dedicated to the single task of performing its safety function. Mention is made of isolation within the DCD and in WCAP 15776 but reference to dedication to single task could not be found.*	*Westinghouse could consider making the compliance against specific sections of chapter 7, for example against section 7.3. Specifically the requirement "Where it is necessary for other functions to be encompassed, the whole system should be classified as a safety system and the safety function should not be jeopardised by the other functions" do not appear to have been addressed*

SAP No.	Main Findings / Observations	TQ Summary
ESS.20	*ESS.20 requires that "Connections between any part of a safety system (other than the safety system support features) and a system external to the plant should be avoided." and the response in the Roadmap does not appear to address the requirements.*	*- The response in the roadmap does not appear to address the requirements for the avoidance of connections to external systems.* *- If connections external to the plant cannot be avoided, for electrical, electronic or computer-based safety systems they should be restricted in function to that of monitoring only, and should incorporate adequate isolation features so that no fault associated with that equipment or its connections would jeopardise the function of the safety system. Could Westinghouse indicate where this is done, as the response in the roadmap does not appear the address the requirements.*
ESS.23	*The AP1000 roadmap does not argue satisfactorily that the AP1000 meets the SAPs.*	*- The response is incomplete for SAP ESS.23 and not all requirements regarding unavailability have been addressed.* *- The response is based on US standards and provides inadequate compliance with UK international and C&I nuclear standards.* *- The retrace within the DCD is too wide to show compliance against the SAP.*
ESS.24	*The AP1000 roadmap does not argue satisfactorily that the AP1000 meets the SAPs.*	*- The response is incomplete for SAP ESS.24 and not all requirements have been addressed.* *- The retrace within the DCD is too wide to show compliance against the SAP for minimal equipment operational requirements.* *- Plant Technical Specifications are identified as specifying limiting conditions for operation.*

SAP No.	Main Findings / Observations	TQ Summary
ESS.27	*The argument for production excellence element of this SAP is largely claimed by reference to the Software Program Manual. However the scope of this does not appear to cover all the software which is defined in the Common Qualified Platform Topical Report WCAP-16097.* *The verification and validation of associated software tools do not meet the requirements of international standards.* *Processes for the acceptance of previously developed software (PDS) do not meet the requirements of international standards.* *The confidence building element of the SAP has not been addressed. Normally this would be the responsibility of the site licensee to address but under the GDA the assessor would expect to see plans for independent evaluation and analysis.*	*- The DCD/PCSR does not provide evidence for the main elements of software production excellence. For example, there does not appear to be any reference to modern software practice e.g. formal mathematical specification, static code analysis or dynamic software testing to meeting the requirements of IEC 60880.* *-The argument for production excellence element of this SAP is largely claimed by reference to the Software Program Manual. However the scope of this does not appear to cover all the software which is defined in the Common Qualified Platform Topical Report WCAP-16097.* *- The software program manual for Common Q systems para 6.3.6.2 states that development tools (compiler, linker loader,) shall not require extensive V&V or testing to qualify their use, since the end product is extensively tested and the tool is not used in on-line operation of the system.* *- Its is not clear how PDS software will be verified.* *-It is not clear how the commercial dedication process CENPD-396-P will meet the requirements of international standards.* *- The confidence building element of the SAP has not been addressed.*
ERL.3	*There is insufficient argumentation and evidence to demonstrate that all sub-claims will meet UK requirements in this area.*	*There appears to be a high level of automation in the C&I and protection systems which provides some of the evidence required to demonstrate the requirements of ERL.3*
EES - Essential Services		
EES.1	*There is insufficient argumentation to demonstrate that the SAP has been satisfied.*	*More argumentation and information is required to demonstrate compliance with this SAP*
EES.2	*There is insufficient argumentation to demonstrate that the SAP has been satisfied.*	*More argumentation and information is required to demonstrate compliance with this SAP*
EES.8	*The SAP is not applicable for the reasons provided in the RP response to the TQ … (Note that clarification of the provision of external electrical power sources is considered in EES.2)*	*N/A*

SAP No.	Main Findings / Observations	TQ Summary
EES.9	*Westinghouse claims that the SAP is not applicable. As part of the step 2 evaluation consideration was deferred to step 3. There is some information with the DCD on uninterruptible power supplies and diesel generators but no information concerning other services*	*Section 8.3.1 of the DCD covers electrical power but provision of other services required for C&I could not be found. Westinghouse are requested to clarify where in the PCSR/DCD the provision of other services is described to support the claim above.*
ESR - Safety Related Systems		
ESR.1	*It is not clear how the US standards relate to the international standards.* *There is insufficient reference information provided within the roadmap to include indicating and recording instrumentation and controls as appropriate.*	*Information is requested on how the US standards relate to international standards and for further information to be provided on recording instrumentations and controls.*
ESR.3	*Westinghouse shall provide specific, rather than general, references to the sections within the AP1000 documentation that presents arguments that show how SAP ESR.3 is satisfied. Evidence of compliance to standards relevant to SAP ESR.3 should be provided.*	*The current references to DCD Chapter 7, 16 and 19 do not provide specific references that point to information that allows the assessor to determine that SAP ESR.3 has been satisfied in terms of arguing "adequate and reliable controls should be provided to maintain variables within specified ranges".*
ESR.4	*The SAP is broadly satisfied but a clarification is sought on the content of DCD description provided.*	*Further information is required on the minimum C&I needed to operate the plant and the clear specification of C&I in order to demonstrate that all sub claims are met in full.*
ESR.5	*Further information is required to confirm that the standards applied on the project are consistent with the requirements of relevant IEC standards.*	*The DCD indicates that a number of IEEE standards have been applied. The assessor has identified a number of IEC standards relating to system, software and hardware requiring the standards applied on the project are confirmed that they are consistent with the relevant IEC standards.*
ESR.7	*SAP ESR.7 is satisfactorily argued within the by traceability through the Roadmap UKP-GW-GL-710 through to the DCD and PCSR. Evidence of design can be found in the DCD Section 9.5.2.*	*N/A*
Other high priority SAPs		
EHA.10	*The AP1000 roadmap does not argue satisfactorily that the AP1000 meets the SAPs.*	*- A coherent response to the EMC requirements of EHA.10 is needed.* *- C&I systems are not identified and so design evidence cannot be reviewed.* *- Requirements for emission limits, immunity and protective measures are not specifically identified.*

SAP No.	Main Findings / Observations	TQ Summary
EHF.7	*DCD section 18.8 provides details of the interface design that appear to be compliant with SAP*	*N/A*
ELO.1	*The AP1000 roadmap does not argue satisfactorily that the AP1000 meets the SAPs.*	*- The retrace within the DCD is too wide to show compliance against the SAP ELO.1 for issues relating to access.* *- Specific information relating to C&I are not identified and so design evidence cannot be reviewed.* *- The use of ALARA has been used and was not justified as ALARP as per SAP guidance.*
EQU.1	*Of the 3 sub-claims, there is not enough evidence to claim that 2 are satisfied.*	*Narratives of qualification programs have been identified but more argumentation and information is required to demonstrate full compliance with this SAP for C&I.*

Annex 3 – Main Observations of the TSC's Architecture Review

This annex reproduces below the main observations from the TSC report "NII GDA Technical Review – C&I System Architecture Functional Safety Review Report for Westinghouse AP1000 – 36331/35796R, Issue 1.4.", Ref. 14.

> *"115 observations have been raised, which are documented in 23 TQs … .The observations have been collated into the main topic areas as follows;*
>
> *Defence in Depth*
>
> *As Westinghouse have not provided an overall requirements specification for the design of the C&I architecture, the assessment has been unable to ascertain the overall suitability of the design intent with respect to design for Defence in Depth. Furthermore, as detailed design has not been finalised in some areas and is therefore unavailable for review, it has not been possible to conclude the assessment of the Defence in Depth design features. No evidence of redundancy in the design of the remote shutdown workstation or back up Human Machine Interface (HMI) systems for the Primary Shutdown System Panel (PDSP) and Secondary Shutdown System Panel (SDSP) could be found. There is a lack of evidence in support of any proposed additional measures to mitigate the consequences of severe accidents.*
>
> *Failure mode management including Common Cause Failure (CCF)*
>
> *Evidence has been found of a potential for demand conflict during actuations within the CIM modules of the PMS as a result of connections to the PLS. No evidence could be found of an analysis of the single failure criterion for each member of each safety group. These issues require further assessment of the design suitability for failure mode management.*
>
> *Evidence of interconnections has been found within the Protection and Monitoring System (PMS) architecture which are a potential source of CCF. No evidence could be found of an evaluation of the effectiveness of measures used to reduce the sensitivity of safety groups to CCF. No evidence was discovered of the Turbine Control System (TOS) platform and implementation; this is also required to allow a complete assessment against CCF.*
>
> *A complete assessment of the C&I systems, in particular the Diverse Actuation System (DAS), TOS and C&I architecture associated with the Boron Injection System has not been possible as no detailed design has been provided in the submission. Furthermore the fail safe principle of operation for the DAS requires further assessment.*
>
> *Independence and diversity*
>
> *Evidence has been found of systems of different classification sharing common resources, e.g. PLS Ovation interfaces and gateway devices contained in PMS cabinets. Additionally there is a lack of evidence of information on cyber-security and networks, the assessment has been unable to ascertain the adequacy of independence and diversity features. There is a lack of information for the Safety/Qualified Data Processing System (QDPS) displays on the PDSP and SDSP and the Data Display and Processing System (DDPS), these issues have impeded assessment of the independence and diversity features. No evidence could be found of any techniques used to minimise the risk and consequences of failure propagation and side effects of failures. Limited evidence was found of hazard assessments for all safety and safety related systems.*
>
> *Provision for automatic and manual safety actuation*
>
> *There is a lack of evidence for consideration given to the choice of manual or automatic safety actions beyond the period of "the 30 minute rule". No evidence could be found to establish that the operator has sufficient information available to take a correct course of action when making decisions for appropriate manual control; e.g. to allow the operator to determine the cause of accidents and executing plant emergency plan. It is also unclear how the operator safely shuts down the plant when*

the operator displays have failed. These issues have impeded assessment of the automatic and manual safety actuation design features.

Appropriateness of equipment type/class

It was determined that Westinghouse considered the QDPS to be a Class 2 system, however it provides manual and automatic indications and controls that are part of the Category A safety functions. The QDPS should therefore be considered to be a Class 1 system. The DAS has been claimed as a non-safety system and Westinghouse have assigned it as Category B Class 2; however the DAS is presented as part of the safety group and should be considered to have a Category A function. Exact alignment of the Westinghouse classification system, used within the design with that defined by IEC 61226 has not been established, e.g. in the Westinghouse response to the NII TQ ref TQ-AP1000_000007, the DAS is indicated as a Class B system. The appropriateness of the classification of C&I systems have therefore not been confirmed by the assessment. This is due to the lack of evidence on safety requirements and corresponding functions with their categorisation and their apportionment to the safety systems of the associated safety group. These issues require further assessment of the appropriateness of the equipment type/class provided in the design submission.

General Findings

The reliability data provided by Westinghouse for the PMS, Plant Control System (PLS) and DAS has not been substantiated and evidence has been requested. No evidence of a fault schedule for the PMS and DAS could be found. No evidence was found of standards alignment or compliance tables between US and International standards requirements. No evidence could be found of the tools used to assure consistency of data exchanged between C&I systems or confirmation that the operational behaviour of the PMS and DAS is free of unintended dependencies from any external influences."

Annex 4 - Main Observations of the TSC's Diversity Review

This annex reproduces below the main observations from the TSC report "NII GDA Technical Review – C&I Diversity Aspects of C&I Category A Functional Systems Design Assessment for AP1000 – 36331 / 35867R, Issue 1.7." Ref. 15.

> *"55 individual questions / observations have been raised by the review. These have then been grouped into nine topic areas. Each topic is documented in a Technical Query (TQ). The nine topic areas and a summary of the observations are presented below:*
>
> 1 *Analysis of Common Cause Failure: A claim is made that Common Cause Failure (CCF) between the PMS and DAS is either not plausible, due to the diversity between the two systems, or so unlikely that it does not affect the probabilistic claim being made on the two systems in combination. Additional arguments and evidence are required in support of this claim.*
>
> *This topic also covers manual backups with respect to analysis of CCF. The rationale for inclusion / non-inclusion of manual backups within each system (PMS and DAS) is unclear. No analysis could be found of the susceptibility of the automatic and manual PMS and DAS functions to dependent and common mode failures.*
>
> 2 *The coverage (in terms of functionality) of the DAS is dependent on the claim made on the PMS. A sensitivity study has been carried out by Westinghouse which demonstrates that a reduced claim on the PMS does not have a significant effect on the overall plant risk, and does not affect the ability of the AP1000 to meet the risk targets. The AP1000 is therefore to be assessed against the reduced claim. Arguments and evidence are required to confirm that the diverse coverage of the DAS (in terms of functionality) is adequate to ensure that the plant safety targets are met in light of the reduced claim.*
>
> 3 *Functional diversity and equipment diversity: No analysis exists demonstrating functional diversity and equipment diversity across each safety group where diversity is claimed.*
>
> - *Functional diversity: No claims, arguments and evidence could be traced relating to diversity between the C&I safety systems for reactor shutdown; i.e. control rods and boration.*
> - *Equipment diversity: It is noted that Field Programmable Gate Array technology is used for carrying out logic and I/O functionality within the Component Interface Modules of the PMS, and is also used extensively within the DAS. No claims, arguments or evidence of the acceptability of this with respect to requirements for diversity could be traced.*
>
> 4 *Independence and segregation: No evidence could be traced that safety groups have been defined, or that the independence of the risk reduction mechanisms within each safety group (including services and communications), or of the hardware actuated, has been assessed. No evidence could be traced that segregation between each safety system constituent has been assessed.*
>
> 5 *Maintenance and test: No evidence could be found that the behaviour of the PMS and DAS during maintenance and test activities has been assessed to demonstrate independence such that maintenance or test of one system does not have an adverse effect on the other.*
>
> 6 *Verification and validation: There is no evidence of the intention to use diverse verification and validation (V&V) procedures or methods for the PMS and DAS systems. There are also some specific requirements for V&V activities (originating in the Standards and related documents) which are not covered in the V&V documentation currently available.*

7 *General: A number of general observations are made, arising from the assessment, but not necessarily linked to diversity between the PMS and DAS. These are recorded to avoid oversight.*

8 *Probabilistic and deterministic analysis of safety groups:*

- *There is no evidence of a probabilistic and deterministic assessment of each safety group. There is likewise no evidence of a diversity assessment for each safety group where both the PMS and DAS are claimed, or evidence that such an assessment has been used to influence claims on the PMS and DAS in combination.*

- *It is not clear how Westinghouse plan to ensure a successful outcome from assessment using TAG 003. There is no evidence of an analysis in line with TAG 003 6.2 ii) and iii) which covers deterministic requirements to be applied for all faults where the safety systems (SS) require a failure per demand (fpd) of between 1E-2 and 1E-6.*

- *There is no evidence that Westinghouse has studied (probabilistically and deterministically) situations where the PMS and DAS are claimed as redundant risk reduction mechanisms which actuate the same component.*

9 *Additional diversity issues: Various topics relating to diversity between the PMS and DAS are covered, including:*

- *Guidance for assessment of compliance with SAP ESS.27 is given in TAG 046. It is not clear how Westinghouse plan to ensure a successful outcome from assessment using TAG 046. The UK considers that the DAS cannot be classified as a simple hardware based system. The development process for an FPGA based system has a lot in common with a "computer based system" development and in that context the guidance of TAG 046 is applicable.*

- *The DAS should be regarded as "complex hardware" in accordance with SAP ESS.21 and will need to address SAP paragraph 355.*

- *It is not clear whether identical hardware and /or software components have been used across the PMS and DAS.*

- *There is no evidence that the PMS and DAS have been analysed for susceptibility to common triggers."*