Office for Nuclear Regulation

An agency of HSE

Generic Design Assessment – New Civil Reactor Build

Step 4 Control and Instrumentation Assessment of the Westinghouse AP1000® Reactor

Assessment Report: ONR-GDA-AR-11-006
Revision 0
11 November 2011

COPYRIGHT

First published December 2011

PREFACE

The Office for Nuclear Regulation (ONR) was created on 1st April 2011 as an Agency of the Health and Safety Executive (HSE). It was formed from HSE's Nuclear Directorate (ND) and has the same role. Any references in this document to the Nuclear Directorate (ND) or the Nuclear Installations Inspectorate (NII) should be taken as references to ONR.

The assessments supporting this report, undertaken as part of our Generic Design Assessment (GDA) process, and the submissions made by Westinghouse relating to the AP1000® reactor design, were established prior to the events at Fukushima, Japan. Therefore, this report makes no reference to Fukushima in any of its findings or conclusions. However, ONR has raised a GDA Issue which requires Westinghouse to demonstrate how they will be taking account of the lessons learnt from the events at Fukushima, including those lessons and recommendations that are identified in the ONR Chief Inspector's interim and final reports. The details of this GDA Issue can be found on the Joint Regulators' new build website www.hse.gov.uk/newreactors and in ONR's Step 4 Cross-cutting Topics Assessment of the AP1000® reactor.

EXECUTIVE SUMMARY

My report presents the findings of the Control & Instrumentation (C&I) assessment of the AP1000 reactor undertaken as part of Generic Design Assessment (GDA) Step 4 of the Health and Safety Executive's (HSE) GDA. I carried out my assessment using the Pre-Construction Safety Report (PCSR) and supporting documentation submitted by Westinghouse Electric Company (WEC) during GDA Step 4.

My assessment has followed a step-wise-approach in a claims-argument-evidence hierarchy. In GDA Step 2, the claims made by WEC were examined; in GDA Step 3, the arguments that underpin those claims were examined.

The scope of the GDA Step 4 assessment was to review the safety aspects of the AP1000 reactor in greater detail, by examining the evidence, supporting arguments and claims made in the safety documentation. The GDA Step 4 assessment builds on the GDA Steps 2 and 3 work, and provides a judgement on the adequacy of the C&I information contained within the PCSR and supporting documentation.

It is seldom possible, or necessary, to assess a safety case in its entirety; therefore, sampling is used to limit the areas scrutinised, and to improve the overall efficiency of the assessment process. Sampling is performed in a focused, targeted and structured manner with a view to revealing any topic-specific or generic weaknesses in the safety case. To identify the sampling for the C&I an assessment plan for GDA Step 4 was set-out in advance.

My assessment has focussed on the:

- arguments and evidence presented for compliance to the HSE C&I Safety Assessment Principles (SAPs);
- main design and implementation standards for all C&I safety and safety related equipment (i.e. the Systems Important to Safety (SIS));
- WEC's safety case for selected key C&I SIS and platforms used to implement the systems (e.g. covering the safety Class 1 Protection and safety Monitoring System (PMS) and safety Class 2 Diverse Actuation System (DAS));
- C&I architecture including defence in depth, independence and diversity; and
- diversity of those systems contributing to implementation of the highest category safety functions (i.e. the PMS and DAS);

A number of items have been agreed with WEC as being outside the scope of the GDA process and hence have not been included in my assessment.

From my assessment, I have concluded that:

- the PCSR and supporting documentation cover the main C&I SIS expected in a modern nuclear reactor;
- based on review of the standards implemented by WEC for the selected key C&I SIS and WEC's standards conformance submission, the C&I standards are broadly in accordance with those expected in the nuclear sector;
- WEC's safety cases for the PMS and DAS are in general accordance with our expectations (noting that further implementation detail needs to be added to the safety cases following design completion); and
- the overall C&I architecture is generally in accordance with expectations.

In some areas there has been a lack of detailed information that has limited the extent of my assessment. As a result I will need additional information to underpin my conclusion and these are identified as Assessment Findings to be carried forward as normal regulatory business, such as standards compliance demonstration for SIS (covering the full lifecycle) and detailed analyses of the diversity between the PMS and the Plant Control System (PLS). These are listed in Annex 1.

Some of the observations identified within this report are of particular significance and will require resolution before HSE would agree to the commencement of nuclear safety related construction of an AP1000 reactor in the UK. These are identified in this report as GDA Issues and are listed in Annex 2. In summary, these relate to:

- changes made to the DAS architecture (i.e. from two-out-of-two actuation voting to two-out-of-three / dual one-out-of-two) to significantly improve fault tolerance and availability during plant operation;
- change of DAS technology from being based on complex Field Programmable Gate Arrays (FPGAs) to non-programmable electronics in order to address a major concern on DAS and PMS / Component Interface Module (CIM) diversity;
- provision of detailed diversity analyses (PMS / DAS and PLS / DAS) which need to be undertaken as a consequence of the DAS technology change;
- provision of equipment to reduce the frequency of spurious Automatic Depressurisation System (ADS) operation in the event of PMS failure;
- fully defining the approach to the justification of smart devices (based on computer technology) used in SIS and provision of a programme showing when implementation evidence will be available;
- enhancements to the safety cases for the PMS (including the AC160 platform and CIM used by the PMS), and the DAS;
- provision of safety cases for the safety related Class 2 / 3 Distributed Control and Information System (DCIS) (comprising the PLS and Data Display and processing System (DDS)) and Ovation platform that fully meet expectations; and
- provision of safety Class 1 displays and controls outside of the Main Control Room.

Overall, based on the sample undertaken in accordance with Nuclear Directorate (ND) procedures, I am broadly satisfied that the claims, arguments and evidence laid down within the PCSR and supporting documentation submitted as part of the GDA process present an adequate safety case for the generic AP1000 reactor design. The AP1000 reactor is therefore suitable for construction in the UK with respect to the adequacy of the C&I, subject to satisfactory progression and resolution of GDA Issues to be addressed during the forward programme for this reactor and assessment of additional information that becomes available as the GDA Design Reference is supplemented with additional details on a site-by-site basis.

LIST OF ABBREVIATIONS

ABB	Asea Brown Boveri
AC 160	Advant Controller 160
ADS	Automatic Depressurisation System
ACC	AMPL Configuration Control
AFI	Areas For Improvement
ALS	Advanced Logic System
AMPL	ABB Master Programming Language
AOV	Air Operated Valve
AQD	Add Quality Demonstration
AQE	Added Quality Exercise
ASN	L'Autorité de sûreté nucléaire (French Regulator)
BMS	(Nuclear Directorate) Business Management System
BPL	Bistable Processor Logic
BSC	Basis of Safety Case
C&I	Control and Instrumentation
CAE	Claims-Argument-Evidence
CBSIS	Computer Based System Important to Safety
CCF	Common Cause Failure
CIM	Component Interface Module
CM	Compensating Measures
CMF	Common Mode Failure
CMT	Core Make-up Tank
COTS	Commercial Off The Shelf
DAS	Diverse Actuation System
DCIS	Distributed Control and Information System
DCP	Design Change Process
DDS	Data Display and processing System
DLCE	Design Life Cycle Evaluation
EDCD	European Design Control Document
EMC	Electromagnetic Compatibility
ESF	Engineered Safety Features
FPGA	Field Programmable Gate Array
FQAJ	Final Quality Assessment and Justification Report
GDA	Generic Design Assessment
GOHE	Generic Operating History Evaluation
HDL	Hardware Description Language

LIST OF ABBREVIATIONS

HSE	The Health and Safety Executive
HSL	High Speed Link
IAEA	The International Atomic Energy Agency
ICBM	Independent Confident Building Measures
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IIS	In-core Instrumentation System
ILP	Integrated logic Processor
IRWST	In-containment Refuelling Water Storage Tank
IV&V	Independent Verification and Validation
LCL	Local Coincidence Logic
MCR	Main Control Room
MDEP	Multinational Design Evaluation Programme
MOV	Motor Operated Valve
MTBF	Mean Time Before Failure
ND	Nuclear Directorate
NEA	Nuclear Energy Agency
NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
OCED	Organisation for Economic Co-operation and Development
OCS	Operation and Control centres System
ONR	Office for Nuclear Regulation
PC	Personal Computer
PCEC	Programmable Complex Electronic Component
PCSR	Pre-Construction Safety Report
PE	Production Excellence
pfd	Probability of failure on demand
PIE	Postulated Initiating Event
PLC	Programmable Logic Controller
PLS	PLant control System
PMS	Protection and safety Monitoring System
PSA	Probabilistic Safety Analysis
PSQ	Product Software Qualification
QA	Quality Assurance
QAP	Quality Assurance Programme
QDPS	Qualified Data Processing System
QMS	Quality Management System

LIST OF ABBREVIATIONS

RGA	Risk Gap Analysis
RI	Regulatory Issue
RMS	Radiation Monitoring System
RO	Regulatory Observation
RP	Requesting Party
RRAS	Repair Replacement and Automation Services
RSR	Remote Shutdown Room
SAP	Safety Assessment Principles
SCA	Software Criticality Analysis
SCI	Safety Criticality Index
SCM	Safety Case Map
SFC	Single Failure Criterion
SIS	Systems Important to Safety
SMS	Special Monitoring System
SRNC	Safety Remote Node Controller
SRS	Safety Related System
SS	Safety System
SSD	System Specification Document
STUK	Sateilyturvakeskus, the Finnish regulator
TO	Technical Observation
TOS	Turbine Operating System
TQ	Technical Query
TSC	Technical Support Contractor
UK	United Kingdom
US	United States
USA	United States of America
V&V	Verification & Validation
WEC	Westinghouse Electric Company LLC

TABLE OF CONTENTS

Tables

Annexes

1 INTRODUCTION

1 My report presents the findings of the Generic Design Assessment (GDA) Step 4 Control & Instrumentation (C&I) assessment of the AP1000 reactor Pre-Construction Safety Report (PCSR) (Ref. 22) and supporting documentation provided by Westinghouse Electric Company (WEC) under the Health and Safety Executive's (HSE) GDA process. Assessment was undertaken of the PCSR and the supporting evidentiary information derived from the Master Submission List (Ref. 23). The approach taken was to assess the main submission (i.e. the PCSR) and then undertake assessment of the relevant documentation sourced from the Master Submission List on a sampling basis in accordance with the requirements of Nuclear Directorate (ND) Business Management System (BMS) procedure AST/001 (Ref. 2). I used the Safety Assessment Principles (SAPs) (Ref. 4) as the basis for my assessment. Ultimately, the goal of assessment is to reach an independent and informed judgment on the adequacy of a nuclear safety case.

2 During the assessment a number of Technical Queries (TQ), topic meeting actions, and Regulatory Observations (RO) were issued and the responses made by WEC assessed. Where relevant, detailed design information from specific projects for this reactor type has been assessed to build confidence and assist in forming a view as to whether the design intent proposed within the GDA process can be realised.

3 A number of items have been agreed with WEC as being outside the scope of the GDA process and hence have not been included in my assessment. These are identified in Section 2.3.5 of this report.

2 NUCLEAR DIRECTORATE'S ASSESSMENT STRATEGY FOR C&I

4 My GDA Step 4 assessment strategy for the C&I topic area was set out in an assessment plan (Ref. 1) that identified the intended scope of the assessment and the standards and criteria that would be applied. This is summarised below.

2.1 Assessment Plan

5 The objective of the GDA Step 4 assessment was to review the safety aspects of the proposed C&I design by examining the evidence supporting the arguments and claims made in the WEC AP1000 safety documentation. The GDA Step 4 assessment builds on the GDA Steps 2 and 3 work, and provides a judgement on the adequacy of the C&I safety demonstration contained within the PCSR and supporting documentation.

6 My GDA Step 4 assessment examined the remaining claims not previously assessed (e.g. addressing relevant HSE SAPs not previously considered) and the underpinning arguments. However, the scope of this assessment was primarily concerned with examination of samples of the 'evidence' to support claims for all HSE SAPs within the scope of assessment. For C&I 'evidence' was broadly interpreted as including:

- the detailed documentation to demonstrate conformance with the HSE SAPs (i.e. how the HSE SAP goals are met);
- the detailed documentation to demonstrate compliance with the standards for the equipment, production processes and safety justification;
- information substantiating the C&I functionality and reliability claims; and
- information supporting production excellence claims for the pre-existing platforms.

7 My GDA Step 4 assessment included assessment of the processes to be used to produce and justify the application specific software and hardware for the Safety Systems (SS) and Safety Related Systems (SRS) (i.e. the Systems Important to Safety (SIS)). The actual Protection and safety Monitoring System (PMS) application code was not available for assessment during GDA Step 4 (WEC declared this to be out of scope).

8 My GDA Step 4 assessment examined the 'final' version of the PCSR (Ref. 25) delivered in March 2011 to determine any impact on the conclusions of the assessment completed to that point (Ref. 96). My assessment in GDA Step 4 included verification that all matters that have been resolved were suitably dealt with in the submission / consolidated PCSR (Ref. 25). I found that the consolidated PCSR does not make use of or reference much of the information provided in response to such matters (e.g. Regulatory Observations), consequently it falls short of expectations. Cross cutting GDA Issue **GI-AP1000-CC-02** has been raised to progress concerns related to the adequacy of the consolidated PCSR (see ND Assessment Report ONR-GDA-AR-11-016, Ref. 97).

2.2 Standards and Criteria

9 The standards and criteria that were used to judge the AP1000 C&I were HSE SAPs (Ref. 4), Technical Assessment Guides (TAGs), and relevant international standards and guidance (e.g. Ref. 5). Table 4 identifies the HSE C&I SAPs considered during the C&I assessment.

10 ND's C&I TAGs provide further guidance for some of the HSE C&I SAPs. The key TAGs are T/AST/003 (Ref. 8) for SSs and T/AST/046 (Ref. 9) for systems containing computer /

complex technology. The majority of the C&I SIS deployed on the AP1000 contain such technology.

11 The standards and criteria used for the C&I GDA Step 4 assessment include relevant nuclear sector standards related to C&I system level design, system architecture and diversity of systems (e.g. Refs 10 to 13, 17 to 19, 28 and 30). Other significant guidance includes the report of the seven party task force on safety critical software (Ref. 5) and the report on the use of computers in safety critical applications (Ref. 15).

2.3 Assessment Scope

12 The C&I GDA Step 4 assessment scope included the specific elements shown below.

- Completion of the technical review of WEC's responses to the ND GDA Step 3 C&I Assessment Report observations (Ref. 6). This includes topics such as categorisation of functions, classification of systems, compliance to International Electrotechnical Commission (IEC) C&I SIS standards and special case procedure for computer-based systems (Ref. 9).
- Review of the "arguments" and "evidence" made for compliance to the HSE C&I SAPs (Ref. 4) (i.e. completion of the claims-arguments-evidence based review against the SAPs).
- Review of the main design and implementation standards for all C&I SIS (Class 1, 2 and 3). The sampling of the detailed evidence during GDA Step 4 (e.g. to demonstrate the standards have been adequately applied) predominately focused on the Class 1 SSs (e.g. reactor protection) and the key Class 2 SIS.
- Review of WECs' safety case for the Class 1 (e.g. ABB AC 160) and key Class 2 SIS platforms and pre-developed components using appropriate guidance and standards.
- Review of the safety case for the implementation of the Class 1 and key Class 2 SIS (e.g. development of application code, Independent Verification and Validation (IV&V) and confidence building measures etc.) using the pre-developed platforms and equipment selected by WEC.
- Further review of the C&I architecture including provision for defence in depth, independence and diversity, provisions for automatic and manual safety actuations and appropriateness of equipment class.
- Further review of the diversity of systems that implement Category A functions (e.g. PMS and Diverse Actuation System (DAS)).
- Review of the impact of PCSR revisions.

2.3.1 Findings from GDA Step 3

13 The findings of my GDA Step 3 Assessment Report (Ref. 6) are summarised below.

- WEC had produced a PCSR and supporting documentation that addressed the main C&I systems expected in a modern nuclear reactor but the safety case argumentation needed improvement.
- While the AP1000 C&I architecture was not unacceptable further assessment of the sensitivity of overall risk to changes of the PMS and the DAS reliability figures was necessary. This may lead to the need to review the C&I architecture.

- Further substantiation was required to support the classification of the DAS, its contribution to the safety groups that implement Category A (reactor protection) functionality, and the adequacy of the diversity between the DAS and PMS.
- The DAS design was 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 PMS application code is within GDA scope and will be included in the GDA Step 4 assessment.

14 No Regulatory Issues (RI) or ROs were raised in respect of the C&I during GDA Step 3. Assessment of WEC's responses to the findings of the GDA Step 3 Assessment Report is provided in the Sections below.

2.3.2 Additional Areas for GDA Step 4 C&I Assessment

15 My GDA Step 4 assessment includes completion of the review of HSE C&I SAPs considered appropriate for sampling during assessment of a new reactor design. Therefore, there is an increase in the number of HSE SAPs reviewed during GDA Step 4 compared to that assessed during GDA Step 3. In addition, GDA Step 4 includes sampling of the detailed evidence used to substantiate safety case claims.

16 During GDA Step 4 the assessment scope was widened to include coverage of the C&I standards for Class 1, 2 and 3 SIS, a review of key C&I platforms (e.g. AC 160 and Ovation) and a review of the processes used to develop applications for SIS using these platforms.

2.3.3 Use of Technical Support Contractors

17 A Technical Support Contractor (TSC) was engaged to assist with the C&I assessment work in GDA Step 3, and the same contractor assisted during GDA Step 4. The scope of work undertaken by the TSC included:

- sample-based review of the evidence used to demonstrate compliance to HSE C&I SAPs;
- sample-based review of the main design and implementation standards used for all C&I SIS equipment (e.g. AC160, Ovation and smart devices);
- sampling of the detailed design and implementation evidence of the Class 1 platform (AC 160) and Class 2 platforms (WEC 7300 series equipment and Ovation);
- sampling of the detailed evidence of the implementation methods for Class 1 SS (PMS), Class 2 SS (DAS) and the key Class 2 SRSs (e.g. Plant Control System (PLS));
- sampling of the detailed evidence of C&I architecture safety capability, including a review of the overall system integration;
- sampling of the detailed evidence of the diversity of the platforms (AC 160 and 7300 series) and systems (PMS and DAS) that implement Category A functions; and
- review of the possible contribution of the platforms and SIS to Common Cause Failure (CCF) of Category A functions.

18 The TSC undertook detailed technical reviews under the close direction and supervision of ND. The regulatory judgment on the adequacy or otherwise of the AP1000 was made exclusively by ND. ND raised all ROs and TQs with WEC.

19 The TSC has provided GDA Step 4 reports that address the scope of work listed above. The TSC also reviewed responses to ROs, Technical Queries (TQ) and Level 3 meeting Actions placed on WEC. The TSC reports include a summary statement of the results of its work and findings (i.e. Technical Observations (TOs)). The summary statements including all TOs are reproduced in Annexes 3 to 8 of this report. I have reviewed the TSC's TOs and, as considered appropriate, taken them forward under GDA Issues (see Annex 2) or Assessment Findings (see Annex 1). The TSC TOs provide further guidance on the GDA Issues or Assessment Findings and their means of resolution. Within this report references to the TSC TOs are provided using the unique TO identifiers (e.g. T13.TO1.01).

2.3.4 Cross-cutting Topics

20 I address the following Cross Cutting Topics in this report: Smart Devices and Metrication.

21 Smart Devices – WEC needs to fully define the approach to the justification of smart devices (based on computer technology) used in SIS. Smart technology is present in many types of modern equipment such as smart sensors, actuators, electrical protection relays and mechanical packaged plant. It is my expectation that WEC has arrangements that ensure such devices are identified wherever they are used in SIS and are appropriately qualified for their intended use. In relation to smart devices used in C&I SIS, a submission that fully defines an acceptable approach to the justification of smart devices including provision of a programme showing when implementation evidence will be available is required. I have raised a GDA Issue to cover the submission of the justification approach for smart devices and evidence of the implementation of the approach (see Section 4.3). Another concern associated with smart devices is the potential for their use, for a given Postulated Initiating Event (PIE), in multiple lines of defence. A GDA Assessment Finding (see Section 4.5) addresses this concern.

22 Metrication - WEC's design is based on the use of imperial rather than metric units and this has been identified as a cross cutting issue. However, the AP1000 C&I components such as electronic systems' cards, chassis and cabinets are all built to accepted standard sizes such as those defined in the Eurocard IEC 60297 (Ref. 36) and Institute of Electrical and Electronic Engineers (IEEE) 1101 (Ref. 37) standards. Use is also made of standardised connectors conforming, for example, to the IEC 60603 (Ref. 38) standard. As a result the AP1000 C&I components use a mix of imperial and metric units. The AP1000 uses a number of specialist instruments (e.g. neutron flux instrumentation) designed to imperial units. There would be a potential significant safety detriment if the design and qualification of equipment of this type needed to be repeated in order to meet a requirement to base the design of all C&I components on standardised metric units. The equipment enclosures are based on imperial units and WEC has explained (Ref. 39) the potential safety detriment of having to repeat the design and qualification of such equipment. WEC's proposal to retain the existing C&I designs that includes equipment using imperial units is accepted.

2.3.5 Out of Scope Items

23 WEC has identified the scope of its GDA submission (Ref. 26) by reference to the major platforms in terms of their "description" and "qualification" (see Table 1 below). For the major C&I SIS, WEC identified the scope in terms of their status in relation to progress through the development life cycle. The main SIS identified by WEC are the:

- Protection and Monitoring System (PMS);
- Diverse Actuation System (DAS);
- PLant control System (PLS);
- Data Display and processing System (DDS);
- Operation and Control centres System (OCS);
- Radiation Monitoring System (RMS);
- In-core Instrumentation System (IIS);
- Special Monitoring System (SMS); and
- Turbine Operating System (TOS).

24 The availability of evidence is identified as follows:

A – all evidence for that stage of development is complete and available to ND for assessment;

B - the documentation that specifies the process for that phase is available but not all the output products (e.g. documents and reports) from that phase are available to ND for assessment; and

C – neither the documentation that specifies the process nor the output products for that phase are available to ND for assessment.

25 Platforms for the major C&I systems identified by WEC along with availability of documentation for assessment declared in WEC letter 'WEC 00512N' (Ref. 26) are shown in Table 1 below.

Table 1: Platforms for major C&I systems

	Common Q	7300	Ovation	RMS	TP800	IIS	SMS
Platform Description	A	A	A	C	C	C	C
Platform Qualification	A*	B*	B	C	C	C	C

Note

A* The following Common Q components are not qualified to Category A / Class 1 standards: DP620, AI687, AI688, CI631, CI527 and flat panel displays.

B* Original 7300 series qualification documentation will be available but the DAS system will be qualified to the AP1000 requirements before deployment.

26 The AP1000 SIS identified by WEC along with availability of documentation for GDA assessment declared in WEC letter 'WEC00512N' (Ref. 26) are outlined in Table 2 below.

Table 2: AP1000 C&I SIS

	PMS	DAS	PLS	DDS	OCS	RMS	IIS	SMS
Design Requirements	A	B	A	A	A	B	A	A
System Definition	A*	B	B	B	A	B	A*	A
Design	B	B	B	B	B	C	B	B
Implementation	B	B	B	B	B	C	B	B
Test	B	B	B	B	B	C	B	C
Installation	C	B	C	C	C	C	C	C

Note A* some documents will be missing.

27 There are a number of other C&I platforms / systems not explicitly identified in the tables above, some of which are systems important to safety; these platforms / systems are out-of-scope of GDA and include:

- fire protection and detection C&I;
- waste treatment building C&I;
- lifting equipment (polar crane / fuel route) C&I;
- seismic monitoring system;
- elements of fatigue, leakage, loose parts or vibration monitoring C&I;
- sensors and nucleonics including ex-core sensors;
- package plant C&I systems; and
- plant components (e.g. Motor Operated Valves (MOVs), Air Operated Valves (AOV) and actuators).

3 REQUESTING PARTY'S SAFETY CASE

28 WEC provided a number of documents setting out its C&I safety case and a submission outlining where the HSE SAPs are addressed in the documents. The PCSR (Ref. 22) provides an overview of the C&I provisions. However, the main submission that describes the C&I provisions is the European Design Control Document (EDCD) (Ref. 27), which is referenced from the PCSR. The C&I provisions claimed include those that would be expected of a modern nuclear reactor such as:

- SSs (e.g. reactor shutdown systems such as the PMS and DAS);
- plant control and monitoring systems (e.g. PLS that performs functions such as reactor power control);
- Main Control Room (MCR) including the Operation and Control centres System (OCS) supported by the Data Display and Processing System (DDS) with backup via the remote shutdown workstation; and
- communication systems for information transfer within and external to the plant.

29 The WEC PCSR and EDCD mainly describe a conceptual C&I design and WEC explained 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 has also explained that the PMS is based on the Common Q platform. The United States (US) Nuclear Regulatory Commission (NRC) has generically approved this platform. The DAS was to have been based on Field Programmable Gate Array (FPGA) technology using a process approved by the US NRC for a non-reactor protection application. However, a design change has been made (Ref. 40) and WEC analogue 7300 series equipment is to be used for the DAS thereby enhancing its diversity from the PMS.

30 An important aspect of the safety demonstration is the classification of SIS 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 (i.e. Class 1 systems are implemented using higher safety standards). 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. IEEE standards) and US NRC requirements. Two system classifications are used (i.e. safety-related and non-safety related) rather than the four adopted in the UK (Ref. 4) and by the IEC (Ref. 28).

31 The safety case assessed under GDA Step 4 consisted of the PCSR (Ref. 22), WEC responses to ROs and TQs, and submissions provided by WEC under cover of formal correspondence as listed in the Master Submission List (Ref. 23).

4 GDA STEP 4 NUCLEAR DIRECTORATE ASSESSMENT FOR C&I

32 This Section documents the results of my GDA Step 4 C&I assessment and details the GDA Issues and Assessment Findings that I have raised. GDA Issues require resolution before the start of nuclear island safety-related construction of the reactor. Assessment Findings are important to safety but are not considered critical to the decision to start nuclear island safety related construction of the reactor (see Guidance to HSE and Environment Agency Inspectors on the content of; GDA Issues, Assessment Findings, Resolution Plans and GDA Issue Metrics (Ref. 29)). In order to close the GDA Issues and Assessment Findings the related TSC TOs that provide further guidance will also need to be resolved. A unique TSC TO reference is used to identify the TSC's TOs (see the Annexes for the TO detail).

33 The complete GDA Issues and associated actions are formally defined in Annex 2 of this report.

4.1 GDA Step 4 C&I SAP and Safety Case Claims-Arguments-Evidence Assessment

4.1.1 Assessment

34 This Section provides the results of the assessment of the AP1000's conformance to the HSE C&I SAPs and the adequacy of the safety case "Claims-Argument-Evidence" (CAE) trail. This Section also describes the resolution of the GDA Step 3 assessment observations.

35 A list of the HSE SAPs used to assess the adequacy of WEC's safety case argumentation during GDA Step 3 is contained in my GDA Step 3 C&I Assessment Report (Ref. 6). In selecting the HSE SAPs for GDA Step 3 assessment, I paid particular attention to those HSE SAPs considered to have particular relevance to system and architectural design.

36 The GDA Step 3 HSE SAP argumentation assessment provided a number of conclusions. Those addressed in this Section are shown below.

- "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. 93) does not readily identify all the relevant information within the EDCD or PCSR and contains some information that should be in the safety case.
- The EDCD and the PCSR do not always reference the available evidence that supports the claims (e.g. references to the W-CAP documentation supplied).
- The WEC safety case Claims-Arguments-Evidence (CAE) diagrams supplied in support of the PCSR (Ref. 22) require further development to identify detailed evidence in addition to that already referenced in the PCSR / EDCD."

37 The GDA Step 3 Assessment Report HSE SAP assessment conclusions addressed elsewhere in this report (relating to architecture, platforms and/or applications) are shown below.

- The C&I design is not yet complete (e.g. DAS) and this has limited the depth of assessment (see Sections 4.3 and 4.4).

- 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 SAPs (Ref. 4) or BS IEC 61226:2005 (Ref. 13) (now BS IEC 61226:2009 (Ref.28)) (see Section 4.2).
- Standards - Further clarification was required in relation to the standards used by WEC and their alignment to nuclear sector international standards (see Section 4.2).
- Defence-in-Depth - Further clarification was 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. 19)). However, use was made of two digital platforms (i.e. ABB AC 160 and Ovation) and a FPGA based system. The PMS uses the ABB AC 160 platform, the PLS is based on the Ovation platform and the DAS was to be implemented using FPGA technology (see Section 4.5).
- Diversity - Equipment diversity is used across the two digital platforms PMS (ABB AC 160) and PLS (Ovation), and the DAS. Further clarification was required on the extent of functional diversity (see Section 4.6).
- Failure to Safety - Further clarification was required on the fail-safe principle as applied to C&I systems (see Section 4.4).
- Computer Based Systems Important to Safety (CBSIS) - Further clarification was required as to how the independent 'confidence-building' and production excellence legs (Ref. 9) were addressed (see Section 4.4).

38 The majority of my GDA Step 3 HSE SAP assessments resulted in TQs being raised. The responses to the TQs were assessed during GDA Step 4 and open items recorded in the TSC's GDA Step 4 reports as TOs. In addition, the observations raised in my GDA Step 2 Assessment Report have been reviewed and any matters still open have been raised in the TSC reports as TOs.

39 My GDA Step 3 assessment determined that the PCSR (Ref. 22), the principal safety document, makes a series of claims in respect of the C&I systems but presents little in the way of supporting arguments or evidence (i.e. there was no clear CAE trail within the documentation). The EDCD (Ref. 27) and its subordinate references provided the detailed platform information. This information concentrated on a description of the platforms including what they do and how they do it. WEC also provided reports outlining the compliance of the AP1000 development processes with IEEE standards.

40 To improve the HSE SAP conformance CAE trail for the AP1000 C&I safety case, WEC undertook to provide CAE diagrams (i.e. safety case maps (SCMs) outlining the claims, arguments and references for the evidence documents that provide substantiation of the claims). WEC submitted the SCMs in phases. WEC produced a number of SCM revisions to improve the quality of the maps.

41 In order to determine if an adequate safety demonstration (e.g. one including a clear CAE trail) for the AP1000 platforms and SIS had been provided by WEC, an initial review of the SAPs' conformance SCMs and the clause-by-clause statements of compliance with IEC standards was undertaken. This review revealed that there was insufficient linking of the safety case claims, arguments and evidence. Therefore, I requested that WEC provide a Basis of Safety Case (BSC) for the Ovation platform via RO-AP1000-78 (Ref. 41) and PLS / DDS system via RO-AP1000-80 (Ref. 42). This request for improved safety case documentation was subsequently extended with requests for three further BSCs for the:

- PMS and its Common Q platform via RO-AP1000-101 (Ref. 43);
- Component Interface Module (CIM) element of the Common Q platform via RO-AP1000-100 (Ref. 44); and
- DAS with its changed platform (i.e. using WEC 7300 series equipment) via TQ-AP1000-1031 (Ref. 45).

The BSCs supplied by WEC (Refs 46 to 50) outline the applicable safety principles and standards, provide a demonstration of conformance to the defined safety principles and standards, and identify the evidence that substantiates the claims.

42 I provided feedback to WEC on the first drafts of the BSCs via TQs and associated documentation. The five BSC documents represent major submissions delivered some months after the deadline assumed in the original GDA submission plan. These late submissions led to a compression of the time for my assessment and the TSC's review. However, assessment of the BSCs was necessary as they provided the main WEC submission in relation to the adequacy of the major elements of the AP1000 C&I.

43 WEC has undertaken a substantial programme of work to create the BSC documents, which provide a good basis for the more detailed safety case to be delivered post GDA Step 4. Review of the BSCs for the PMS (including the AC 160 platform used by the PMS) and safety Class 1 CIM has revealed that further enhancements are required to the BSCs. In addition, the safety cases for the Safety Related Class 2 / 3 Distributed Control and Information System (DCIS) (comprising the PLS and DDS) and Ovation platform do not fully meet expectations (e.g. when judged against the expectations for a BSC as outlined in Annex 2). I provide further comment on the safety case documentation including the BSCs and identification of related GDA Issues in Sections 4.3 and 4.4.

44 During GDA Step 4, I completed a review of the "arguments" and "evidence" made for compliance to the HSE C&I SAPs (i.e. completion of the claims-arguments-evidence based review against the HSE SAPs). Table 4 provides a list of the HSE SAPs considered during the GDA Step 4 assessment of the adequacy of WEC's safety case argumentation. The TSC's GDA Step 4 report (Ref. 51) presents the results of the TSC's review of the AP1000 C&I's conformance to the HSE C&I SAPs and the adequacy of the safety case claims-argument-evidence trail. The TSC's review also considered WEC's responses to relevant GDA Step 3 TQs and the TSC's GDA Step 3 observations (Ref. 103). The TOs in the TSC's GDA Step 4 report (Ref. 51) record those matters that remain open. Annex 3 provides a summary of the TSC's GDA Step 4 report including a list of the open TOs.

45 The TSC performed an initial review of the adequacy of the CAE trails for 45 of the 84 HSE C&I SAPs (see Table 4) within the assessment scope. The initial review considered the adequacy of i) SAP requirements coverage, ii) argumentation and iii) appropriateness of the identified evidence. The initial review concluded that there are significant areas for improvement in relation to the demonstration of conformance to the HSE SAPs and gave rise to 46 TSC TOs (see T13.TO1.01, and T13.TO2.01 to T13.TO2.45 in Annex 3).

46 Following the initial review, the TSC, as part of the CAE review, undertook a detailed review of the evidence identified as demonstrating conformance to a subset of six of the HSE C&I SAPs. This review identified a number of generic areas for improvement such as the need to address all SIS and platforms, clarity of the argument and appropriateness of the evidence (see Annex 3). In addition, further HSE SAP related evidence reviews were undertaken by topic specific TSC tasks (e.g. of platforms and SIS), covering 27 HSE SAPs. These reviews have resulted in the TSC raising a further 66 TOs (see T13.TO1.02 in Annex 3).

47 Many of the TOs relate to minor issues such as ensuring precise identification of evidence by the use of section numbers when referring to evidence documents. However, there are also substantive matters (e.g. to ensure all HSE SAP clauses are addressed for all SIS and platforms) that need to be addressed.

48 By the end of the GDA Step 4 assessment, the position on the adequacy of safety case argumentation and identification of evidence (e.g. improvement of the PCSR CAE trail) was not fully satisfactory. I have raised an Assessment Finding to cover the provision of an adequate HSE SAP conformance demonstration (i.e. either through the safety case maps (SCMs) or other documentation linked to the various SIS and platform BSCs).

*GDA Assessment Finding: **AF-AP1000-CI-001** - Safety case argumentation and identification of evidence (CAE trail):*

- *The Licensee shall produce a SAP conformance demonstration covering the full scope of SIS and platforms (i.e. by provision of Safety Case Maps for the 84 HSE C&I SAPs or other documentation as considered appropriate).*
- *The Licensee shall ensure that the SAP conformance demonstration is, as appropriate, included in or referenced from the SIS and platform Basis of Safety Cases (BSCs) (see GDA Issues **GI-AP1000-CI-01, 06, 07, 08 and 09** in Sections 4.3 and 4.4).*

For further guidance see T13.TO1.01, T13.TO1.02 and T13.TO2.01 to T13.TO2.45 in Annex 3, T16.TO2.47 and T16.TO2.48 in Annex 6.

[Time: prior to nuclear island safety related concrete.]

49 The provision of the SCMs and BSC documents has provided significant improvement to the safety case documentation. The initial BSC documents submitted by WEC provide a strong indication that completion of the outstanding work to define fully the BSCs together with a robust HSE SAP conformance demonstration should generate a safety case to the required standard. The improvements to the safety case documentation provided by the SCMs and BSC documents have addressed the major concerns identified during GDA Step 3 (i.e. absence of a CAE structure in the PCSR that clearly demonstrates conformance to the HSE C&I SAPs and satisfaction of key safety case claims).

50 I conclude that in broad terms the HSE SAP conformance and safety case documentation is not unacceptable. However, a number of aspects related to GDA Issues and Assessment Findings require resolution (e.g. enhancements to the PMS and DAS BSCs, and provision of BSCs for the PLS, DDS and Ovation platform that fully meet expectations) in order to further improve the safety case including HSE SAP conformance demonstration.

4.1.2 Findings

51 The GDA Issues on the provision of BSCs that are related to this Section (i.e. as defined in Section 4.3 and 4.4) and the Assessment Finding recorded in the Section above are listed in Annex 2 and 1 respectively.

4.2 C&I Systems' Classification and Standards

4.2.1 Assessment

52 My GDA Step 2 and 3 assessment sought to establish the claims WEC were making in respect of functional categorisation and system classification, and the standards and guidance associated with the system classes. I reviewed the WEC Quality Management System (QMS), as relevant to the AP1000 C&I, processes and procedures implementing the standards and guidance.

53 During GDA Step 4, I examined the detailed implementation of the QMS (as relevant to the AP1000 C&I) and WEC's requirements for implementation of C&I standards and guidelines. The assessment included consideration of the relevant HSE SAPs, principally ECS.1 to ECS.5 on safety classification and standards, and EQU.1 on equipment qualification procedures.

54 The C&I TSC's work provided support to my assessment. The description of the scope of work performed by the TSC and the TOs arising from the work are described in a TSC report (Ref. 52). Annex 4 provides a summary of the TSC's work (Ref. 52) that includes all of the TOs.

55 The assessment of adequacy of WEC's company level (i.e. generic rather than project specific) C&I SIS standards was performed in a progressive, logical and thorough manner and was effectively a four-step process as shown below.

1) Determination of the relevant C&I SIS standards (i.e. those defining relevant good practice) considered applicable to WEC's company level standards. This included consideration of relevant HSE SAPs.
2) Identification of the company QMS.
3) Review of the relevant WEC company level standards and identification of differences between these documents and those documents defining relevant good practice.
4) Determination of the significance of observations arising from the review, and consideration of the GDA Issues or Assessment Findings that should be raised to address any concerns.

56 I consider relevant good practice for C&I SIS to be defined in a suite of international standards produced by the IEC based in Geneva. Standards are developed by multi-disciplinary committees and are subject to international review and voting prior to issue. Issued standards are regularly reviewed and revised, as necessary, to address improvements in technologies and techniques.

57 The British technical committee NCE/8 'Reactor Instrumentation' nominates UK technical experts to the IEC committees that develop and maintain the international C&I standards. The IEC standards relevant to this assessment are identified in 'BSi Technical Committee NCE/8 Nuclear Power Plants - I&C Systems, A Guide to Applicable IEC Standards, AFP – v7 – 2008_12_01' (Ref. 31). I also considered relevant HSE SAPs (e.g. EQU.1, ECS.1, ECS.2, and ECS.3) under this aspect of my assessment.

58 The requirement for assignment of functions to categories and systems to class is set out in HSE SAPs ECS.1 and ECS.2. The relevant IEC C&I nuclear sector standard for categorisation of C&I functions is BS IEC 61226 (Ref. 28). BS IEC 61226 essentially uses deterministic criteria to place C&I functions into one of three safety Categories (i.e. A, B, or C) or identify them as non-safety / not categorised.

59 The IEC C&I nuclear sector SIS standards form a hierarchy with the top-level standard, BS IEC 61513 (Ref. 10), covering general requirements for SIS and architectural

requirements. This standard is the nuclear sector equivalent of the generic IEC industry standard on functional safety of electrical / electronic / programmable electronic safety-related systems (see BS EN 61508 - Ref. 53), where safety-related covers all SIS.

60 Sitting below BS IEC 61513 (Ref. 10) in the hierarchy of IEC nuclear sector standards are standards addressing:

- software for CBSIS performing Category A functions (i.e. the highest safety significance), BS IEC 60880 (Ref. 17);
- software for CBSIS performing Category B and C functions, BS IEC 62138 (Ref. 30); and
- hardware design requirements for CBSIS Class 1 and 2 systems, BS IEC 60987 (Ref. 18).

61 In addition to the top-level IEC standards identified above, there are a range of supporting standards, referred to here as level 2 and 3, covering topics such as equipment qualification, requirements in respect of common cause failure, segregation, and instrument and sensor specific standards (see Ref. 31).

62 The use and application of relevant good practice, as defined by international standards, is an essential component of the required safety case for C&I SIS. The Licensee will need to ensure that the requirements of IEC standards not referenced by WEC and as appropriate to the C&I SIS employed in the AP1000, are addressed in the C&I SIS lifecycle. The lifecycle covers design, procurement and implementation processes etc. (see Assessment Findings below).

4.2.1.1 Quality Management

63 The WEC QMS and its arrangements are aligned with ISO 9000. A key objective of the QMS and its supporting arrangements is to demonstrate compliance with US NRC requirements (i.e. Federal Regulations 10 CFR 50 and the associated US NRC Regulatory guides and position statements). The QMS and its arrangements use IEEE standards as their reference point not IEC standards as expected in the UK.

64 The WEC QMS is an enabling system used to control in-house development or the acquisition and deployment of pre-developed equipment. The WEC QMS was not previously examined in detail in this topic area. WEC indicated that all work is done under the WEC QMS and its arrangements for the individual operating units (e.g. Repair Replacement and Automation Services (RRAS) that undertakes the major C&I works). The QMS includes procedures for new C&I development and commercial dedication of pre-developed C&I equipment. The commercial dedication process takes a commercial product (i.e. one not developed to an appropriate safety / safety related standard) and justifies it for use in a safety / safety related role.

65 WEC explained the QMS and its documentation / management structure by reference to a set of diagrams that outlined the quality programme for the WEC NuStart project (Ref. 54). There are no quality plans or programmes available for the UK GDA project (i.e. as there is no UK reactor construction project at this time). The NuStart C&I project plans and programmes have a hierarchical structure and link to the relevant WEC QMS procedures.

66 The NuStart plans identified WEC's C&I application development processes specifically for systems based on the Common Q (AC 160) and Ovation platforms. The development process requirements were traced back to the WEC QMS arrangements, IEEE

standards, regulatory requirements of 10 CFR 50 Part A, and US NRC Regulatory Guides. Technical areas covered by the development processes include lifecycle phases such as design and coding, verification and validation, testing and configuration management. Sections 4.3 and 4.4 present the assessment conclusions on the adequacy of the arrangements in respect of platforms and SIS applications including compliance of WEC processes to key IEC nuclear sector standards.

67 I have identified the need for a UK specific AP1000 C&I Quality Assurance (QA) programme. The UK QA programme will need to address compliance to appropriate IEC standards or standards demonstrated to be equivalent for the C&I SIS.

> *GDA Assessment Finding: **AF-AP1000-CI-002** – The Licensee shall put in place an overarching Quality Assurance Programme (QAP) for the AP1000 C&I Systems Important to Safety development consistent with the WEC Quality Management System that either:*
>
> - *adopts appropriate IEC nuclear sector standards (Ref. 31): or*
> - *uses standards that are demonstrated to be equivalent to the IEC standards (e.g. through demonstrating the equivalence of WEC procedures and processes to the IEC standards).*
>
> *This QAP shall also identify the flow through of requirements to subcontractors (i.e. to instrument and equipment suppliers). For further guidance see T14.TO1.01, T14.TO2.01, T14.TO2.03 and T14.TO2.04 in Annex 4.*
>
> [Time: Long lead item procurement.]

68 I conclude that the WEC QMS arrangement is adequate to support the development of C&I SIS but specific action is needed to demonstrate compliance with IEC nuclear sector standards or the equivalence of WEC procedures and processes with those standards (see Assessment Finding **AF-AP1000-CI-002**).

4.2.1.2 Categorisation and Classification Standards

69 The AP1000 design and its GDA submissions (e.g. PCSR and EDCD) are based on the categorisation and classification approach used in the US. This has two classes, safety related (IEEE Class 1E for C&I) and non-safety. However, there are internal subdivisions often relating to the nature of the system (e.g. civil, mechanical, electrical or C&I).

70 WEC recognised, at an early stage, the UK requirement to demonstrate compliance with IEC nuclear sector standards, particularly BS IEC 61226:2009 (Ref. 28). During GDA Step 3 WEC explained (Ref. 32) how the US approach mapped to that adopted in the UK (i.e. by mapping the systems into the categorisation scheme defined by the IAEA, HSE SAPs and IEC nuclear sector standards). The function Category and system Class table provided in WEC's submission (Ref. 32) showed reasonable alignment with my expectations on this topic. However, there were a number of areas identified during GDA Step 3 (Ref. 6) where further clarification was required (e.g. Class of the DAS and Turbine Operating System, and scope of Class 1 controls and displays).

71 WEC outlined the Category and Class details in a GDA Step 4 submission (Ref. 33) that also identified the level 1 IEC nuclear sector standards applicable to the C&I SIS. The submission (Ref. 33) also identified a number of systems including the SMS and parts of the PLS (metal impact monitor, coolant pump vibration monitor and balance of plant

control) as non-safety related. Further comment on this is provided below (e.g. see GDA Assessment Finding **AF-AP1000-CI-005**).

72 WEC stated that it will complete the categorisation of functions in accordance with its QMS as the design is "finalised". A generic categorisation procedure (Ref.34) for the AP1000 has been set down following a discussion with ND. The WEC scheme for categorisation of C&I functions in this generic procedure is similar to but not identical to that of BS IEC 61226 (Ref. 28). The generic procedure (Tables B1, B2 and B3 in Ref. 34) identifies how the functional categorisation requirements of BS IEC 61226 (Categories A, B and C) are captured in the WEC scheme.

73 The generic procedure (Ref. 34) also relates the Category of function to the Class of system required to implement the functions. The generic procedure allows a relaxation such that Class 3 systems can implement Category B functions. I did not identify any such relaxations during my assessment of the sampled C&I SIS. I provide further discussion on the appropriateness of system Class below (see GDA Assessment Finding **AF-AP1000-CI-004**).

74 WEC provided a submission (Ref. 35) that documents the result of applying WEC's generic categorisation procedure (e.g. it lists the Category of the major functions and Class of the major AP1000 systems).

75 WEC also identified a C&I specific procedure (Ref. 55) for categorisation of functions. The C&I procedure applies to WEC's operating unit (RRAS) that is responsible for the implementation of the AP1000 C&I SIS. The C&I procedure follows, almost verbatim, the requirements of BS IEC 61226 (Ref. 28).

76 The C&I procedure identifies the Class of the AP1000 C&I SIS in more detail. The functional categories and SIS classes meet expectations. The Class 1 PMS implements Category A reactor trip and engineered safeguard features (ESF) functions. The Class 2 DAS also performs Category A reactor trip and ESF functions. The DAS Class is acceptable since it is in accordance with the requirements of BS IEC 61226 (Ref. 28, clause 7.3.2.1). In addition, Class 2 SIS implement the Category B closed loop control functions associated with the nuclear island. The implementation of turbine control functions in a Class 2 system aligns with my expectations. WEC distribute the operator controls and displays across the SIS and assign them to all three categories and classes. The assignments broadly meet expectations. However, the GDA Step 3 observation of a lack of Class 1 display and control equipment other than in the main control room remains unresolved (see GDA Issue **GI-AP1000-CI-10** in Section 4.5).

77 I conclude that the WEC generic procedure (Ref. 34) for the categorisation of functions and classification of systems, and the results of its application (Ref. 35) are broadly in line with my expectations. The approach is developed in a C&I procedure (Ref. 55) where it is shown that the categories of the C&I functions and system classes are consistent with BS IEC 61226 (Ref. 28). I conclude that, the Class of the major C&I SIS and Categories of functions they perform are aligned with the requirements of the HSE SAPs (Ref. 4) and international standards (i.e. BS IEC 61226, Ref. 28 and BS IEC 61513, Ref. 10).

4.2.1.3 Development Standards

78 The identification of applicable development standards was raised by my GDA Step 3 assessment. The major AP1000 C&I SIS (i.e. the PMS, DAS and DCIS) are all implemented using pre-developed platforms. The PMS uses the AC160 platform, the DAS uses WEC 7300 series equipment and the DCIS uses the Ovation platform. The DAS and DCIS were developed to IEEE standards. The original PMS platform

development was undertaken using the prevailing commercial standards. The SISs' application software development processes all comply with the WEC QMS and hence also to IEEE standards. In order to demonstrate that these processes align with the UK expectations, as expressed in the HSE SAPs, TAGs and IEC standards, WEC agreed to undertake (Refs 32 and 33) a number of standards conformance demonstrations.

79 The standards conformance demonstration included:

1) identification of the level 1 (top tier) IEC nuclear sector C&I standards as applicable to each major C&I SIS;
2) provision of a clause-by-clause demonstration of compliance with the five level 1 IEC nuclear sector C&I standards;
3) consideration of a further eleven level 2 (second tier) IEC nuclear sector C&I standards against the similar standards used for AP1000 development; and
4) consideration of other standards identified in the BSI guide to IEC nuclear sector C&I standards (Ref. 31).

80 For demonstration element 1), WEC identified (Refs 32 and 33) the level 1 IEC nuclear sector C&I standards applicable to each of the major C&I SIS (i.e. BS IEC 61226, BS IEC 61513, BS IEC 60880, BS IEC 60987 and BS IEC 62138). The RRAS C&I specific categorisation document (Ref. 55) cross-references the SIS development phases to the applicable US regulatory requirements and IEEE standards. The document also identifies the individual clauses of the relevant level 1 IEC standards against the development phases. However, the procedure does not require compliance with the IEC standards.

81 The standards identified in WEC submissions (i.e. Refs 35 and 55) broadly meet expectations. The appropriate level 1 IEC implementation standards are correctly associated with the different classes of SIS with two clear exceptions as identified below.

- If software is used to implement the Category A RMS main control room HVAC functions, it will be developed to BS IEC 62138. However, BS IEC 60880 is the normal standard used to implement Category A functions in a Class 1 system.
- Hardware for Class 3 computer based SIS is identified as being compliant with BS IEC 60987 whose scope is for the hardware of Class 1 and 2 SIS. Therefore, the standard that WEC adopt is more onerous than the normal expectation but is conservative.

*GDA Assessment Finding: **AF-AP1000-CI-003** – The Licensee shall provide a safety case for the Radiation Monitoring System. The expectation is that the software development should comply with BS IEC 60880 unless it is demonstrated that this is not reasonably practicable and the use of the lower standard for developing software for Category B functions in accordance with BS IEC 62138 is fully justified.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

82 WEC's classification document (Ref. 35) states that control equipment associated with some mechanical handling plant performing Category A and B functions (e.g. in the fuel route) is to be compliant with commercial rather than nuclear SIS standards. The scope of the C&I SIS identified by WEC for inclusion in GDA (see Section 2.3.5) did not include this equipment. Therefore, no assessment of such equipment has been undertaken. However, mechanical handling plant includes items such as the polar crane that performs

nuclear safety related lifts (e.g. of the reactor pressure vessel head). The correct operation of the control and safety systems of such mechanical plant is important in relation to maintenance of plant safety. I have raised an Assessment Finding in relation to the demonstration of the correct classification of this equipment and its compliance with appropriate standards.

> *GDA Assessment Finding: **AF-AP1000-CI-004** – The Licensee shall ensure that C&I equipment installed as part of systems performing Category A or B functions is either:*
>
> - *assigned to a Class 1 or 2 system as appropriate and justified against relevant standards, or*
> - *a justification is provided for assigning a lower or no-safety class.*
>
> *This not only applies to mechanical handling plant but also to any other equipment (for example the polar crane) where C&I equipment important to safety is embedded into or is part of the system.*
>
> [Time: prior to install polar crane.]

83 For demonstration element 2) above, WEC demonstrated compliance of the WEC procedures and processes with the five level 1 IEC nuclear sector C&I standards (i.e. clause-by-clause). This demonstration includes a table of IEC requirements clauses with cross references to WEC procedure, process and product documentation. I reviewed the adequacy of this evidence as part of my assessment of the platforms and systems important to safety. In general, I found that the procedures for Class 1 and 2 SIS align with the IEC standards. However, the demonstration was incomplete as it did not address:

- all clauses;
- operation and maintenance lifecycle phases
- platforms and systems individually; and
- Class 3 systems.

Sections 4.3 and 4.4 below provide further comment on this finding. WEC has provided additional clause-by-clause standards compliance documentation but this came too late for it to be included in the GDA Step 4 assessment.

84 The WEC procedures do not require compliance with IEC standards. The means of providing a comprehensive demonstration of compliance to IEC standards (see above) including addressing the SIS operational and maintenance lifecycle phase is not apparent.

> *GDA Assessment Finding: **AF-AP1000-CI-005** – The Licensee shall produce a comprehensive demonstration of compliance with the five level 1 IEC nuclear sector C&I standards (i.e. BS IEC 61226, BS IEC 61513, BS IEC 60987, BS IEC 60880 and BS IEC 62138) for the AP1000 C&I Systems Important to Safety (SIS). The demonstration shall address: all relevant clauses; the operation and maintenance part of the SIS lifecycle; platforms and systems individually; and Class 3 systems. For further guidance see T14.TO1.01, T14.TO.03 and T14.TO2.04 in Annex 4, and T16.TO2.05 and T16.TO2.10 in Annex 6.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

85 For each of the eleven level 2 IEC nuclear sector C&I standards (demonstration element 3 above) WEC identified (Ref. 33) the "similar" standard used for AP1000 C&I development (see Table 3 below). WEC claim (Ref. 33) that "The similar standards have the same intent as the associated IEC standard and we have not identified any gaps in our compliance with the similar standards". A number of the IEC level 2 (second tier) nuclear sector C&I standards are identified in the C&I procedure (Ref. 55) as being applicable to stages of the SIS development lifecycle and / or to the achievement of functional and non-functional requirements (e.g. segregation and environmental testing). However, the C&I procedure does not require compliance with the IEC standards.

Table 3: IEC Tier 2 C&I Nuclear Standards and US Equivalents Identified by WEC

Topic	IEC Tier 2	US Equivalent
Common Cause Failure	62340	NUREG/CR 6303
Control Rooms and HMI	60964 61771 61839	NUREG-0700 NUREG-0700 NUREG-0700
Remote Shutdown	60965	Reg. Guide 1.68.2
Separation	60709	IEEE 384
Setpoints	61888	Reg. Guide 1.105
Environmental Qualification	60780	IEEE 323
Seismic Qualification	60980	IEEE 344
EMC Qualification	61000 series	61000 series
Periodic Surveillance Testing	60671	IEEE 338

86 For demonstration element 4, the other IEC standards, WEC state (Ref. 33) that 'For level 3 standards, WEC has compared our processes with the intent of these standards and has not identified any gaps'.

87 WEC did not identify evidence to support its claims:

- of the equivalence of the IEEE standards and Regulatory guides with the level 2 IEC nuclear sector C&I standards;
- that no gaps in compliance had been identified in their processes with the standards claimed as "similar" to the IEC nuclear sector C&I standards; or
- that the WEC processes meet the intent of the level 3 IEC nuclear sector C&I standards.

This lack of evidence is not unexpected as the level 2 and 3 IEC nuclear sector C&I standards relate mainly to detailed design and implementation information that will only become available during the latter phases of a project.

*GDA Assessment Finding: **AF-AP1000-CI-006** – The Licensee shall document the evidence supporting the claims (i.e. made in Ref. 33):*

- *of equivalence of the IEEE standards and Regulatory guides with the level 2 IEC nuclear sector C&I standards;*
- *that no gaps in compliance had been identified in WEC processes with the eleven level 2 standards claimed as similar to the IEC nuclear sector C&I standards; and*
- *that the WEC processes meet the intent of the level 3 IEC nuclear sector C&I standards.*

For further guidance see T14.TO2.05 and T14.TO2.06 in Annex 4.

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

88 A number of HSE SAPs relate to system classification and standards (e.g. ECS.1 to 4 and ESR.5). Compliance evidence for ECS.3 was examined and it was determined that there is scope to improve the CAE trail for the HSE SAPs (see GDA Assessment Finding **AF-AP1000-CI-001 in** Section 4.1).

89 WEC undertook a review of the approach required by standards to the security of CBSIS and has proposed a way forward, which is to demonstrate the equivalence of its approach (i.e. based on US Regulation) with the UK government's standard methodology (Ref. 57). The submission of an example SIS security review including comparison to UK requirements was not delivered within the GDA Step 4 timeframe.

*GDA Assessment Finding: **AF-AP1000-CI-007** - Computer Based Systems Important to Safety Security – The Licensee shall:*

- *demonstrate that its Computer Based Systems Important to Safety (CBSIS) security management system aligns with appropriate standards such as ISO/IEC 27001 (Ref. 56); and*
- *implement a CBSIS security assessment methodology that uses, or is equivalent to, the UK Government's standard methodology (Ref. 57).*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

90 I conclude that the WEC QMS, as applicable to the AP1000 C&I, provides necessary but not sufficient requirements for the AP1000 C&I SIS. The company level arrangements will require the addition of UK project specific procedures and instructions. This is required to support and maintain the claims of compliance with IEC nuclear sector standards for categorisation of functions and classification of systems. I will need additional information to underpin my conclusion and the Assessment Findings above identify these requirements.

4.2.2 Findings

91 The GDA Assessment Findings recorded in the Section above are listed in Annex 1 of this report.

4.3 C&I Platforms and Pre-Developed Equipment

4.3.1 Assessment

92 This Section describes the outcome of my assessment of the AP1000 C&I SIS platforms and pre-developed equipment including conformance with the HSE SAPs and IEC standards. Also reported is progress with resolution of the GDA Step 3 observation on the incomplete design and qualification of the platforms.

93 The C&I TSC's work supported my assessment. The TSC report (Ref. 58) describes the TSC's scope of work and the TOs arising from that work. Annex 5 provides a summary of the TSC's report (Ref. 58) including details of the TOs raised.

94 A risk-based approach to assessment was followed with the greatest assessment effort allocated to those platforms and pre-developed equipment performing the most important nuclear safety functions. All assessment was performed on a sample basis.

95 The majority of the AP1000 C&I SIS make use of existing platforms and pre-developed equipment. The three platforms selected for assessment are the:

- Common Q / Advant Controller 160 (AC 160) platform (PMS);
- 7300 series analogue platform (DAS); and
- Ovation platform (PLS and DDS).

96 The main AP1000 Class 1, 2 and 3 C&I SIS make use of these platforms. The Component Interface Module (CIM) is an essential component of the PMS. The CIM includes the CIM priority logic module and Safety Remote Node Controller (SRNC). The CIM uses FPGA technology and it was included in the assessment as a result of its crucial role in resolving actuation demands from the PMS and PLS. WEC changed the DAS platform during GDA Step 4 from a FPGA based platform to the WEC 7300 series analogue equipment to address concerns about diversity between the DAS and CIM. These concerns arose from the use of common FPGA technology in both the CIM and DAS (see Section 4.6).

97 The information made available by WEC for the GDA SIS platform assessment was that relating to platform descriptions and the qualification processes for the three selected platforms. The results of the qualification processes were only available for the Common Q / AC 160 platform (see Table 2 Section 2.3.5).

98 WEC provided some information on other systems including the: IIS; TOS; SMS; and RMS. These were not part of the assessment sample nor were they included in full as part of WEC's declared GDA C&I scope (Ref. 26). As a result the platforms of these systems were not assessed.

> *GDA Assessment Finding:* ***AF-AP1000-CI-008*** *– The Licensee shall ensure a safety case is produced for the: In-core Instrumentation System; Turbine Control System; and Special Monitoring System.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

99 My assessment commenced with a review of the PCSR (Ref. 22) (i.e. the principal safety document). The PCSR makes a series of claims in respect of the C&I SIS platforms but presents little supporting argument or evidence. The detailed platform information was provided in the EDCD (Ref. 27) and its subordinate references. However, this information concentrated on a description of the platforms including what they do and how they do it. The documents did not provide the necessary safety justification. In

particular, the documents did not identify the arguments and evidence that demonstrate satisfaction of the requirements of appropriate safety guidance, principles and standards.

100 I initially sought the safety justification by review of the SCMs provided for the HSE SAPs' conformance demonstration and WEC's clause-by-clause statements of compliance with IEC standards. The HSE SAP conformance and standards compliance information together with responses to TQs requesting further detailed information were insufficient (e.g. see T15.TO1.09 on the SCMs) to identify a CAE trail. For example, the linking of the samples of evidence from the Oskarshamn project to the AC 160 platform claims was not evident.

101 I arranged a series of meetings with WEC to aid my understanding of the platforms and to facilitate access to the evidence that was only available for examination in the presence of WEC staff. I also requested that WEC provide a BSC for each of the four platforms (see Section 4.1). The four BSCs (Refs 46, 48, 49 and 50) formed a significant element of my assessment of the platforms. The BSCs for the CIM (Ref. 48) and the DAS (Ref. 50) were essential for completion of a meaningful assessment of the CIM FPGA and DAS 7300 series platforms (i.e. given the lack of documentation for the CIM and for the DAS following its platform change).

4.3.1.1 Assessment of the Common Q / AC 160 platform

102 The AC 160 platform is a commercially available computer based platform developed by Asea Brown Boveri (ABB) over the last 20 years at its facilities in Turgi, Vasteras and Mannheim principally for high integrity turbine and boiler, control and protection. The AC 160 platform includes: the control PLC, S600 input/output (S600 I/O) cards, communication links, base software and tools for the generation of application software. The BSC describes the platform development as being in accordance with the commercial standards and practices of the time.

103 WEC adopted the AC 160 platform as its Class 1 platform for the implementation of Category A protection and safety monitoring functions in the late 1990s. The AC 160 platform qualification for Class 1 nuclear applications has two significant elements. The first element was produced from the application of the AC 160 platform for reactor protection at the Oskarshamn 1 reactor. WEC, with the assistance of ABB, undertook an Added Quality Exercise (AQE) to establish a nuclear baseline for the AC 160 platform (i.e. version V1.3/0). The second element is the work associated with the US NRC certification of the Common Q platform for use in the USA. The Common Q core is the AC 160 platform with additional equipment including flat panel displays and post accident monitoring equipment.

104 The objective of the Oskarshamn AQE was to demonstrate the suitability of the AC 160 platform for reactor protection applications. This included demonstrating, as far as practicable, that the platform software was compliant with IEC 60880:1986 (Ref. 59) and its supplement (Ref. 60).

105 The AQE commenced with WEC undertaking a 'Suitability Exercise' to determine the suitability of the AC 160 platform for nuclear use. The 'Suitability Exercise' was guided by the output of a software criticality analysis (SCA). The SCA divided the platform software into partitions and assigned each partition a software criticality index (SCI) depending on its importance to safety (e.g. as a consequence of it going wrong). The 'Suitability Exercise' included evaluation of the AC 160's generic operating history (GOHE) and a design lifecycle evaluation (DLCE) as informed by the SCI. WEC concluded that the platform (i.e. the commercial product AC 160 V1.2) was suitable, in principle, to support a

Class 1 SS. However, a number of open items (e.g. gaps in compliance with IEC 60880:1986) had to be resolved before the AC 160 could be used for nuclear applications.

106 The 'Suitability Exercise' was followed by the implementation of compensatory measures that addressed the open items and created a nuclear baseline. The compensatory measures included the following elements:

- 'Added Quality Demonstration';
- 'Software Modifications';
- 'Design Restrictions' on the use of the platform; and
- 'Additional Steps' (e.g. common cause failure evaluation and independent oversight).

107 The Added Quality Demonstration (AQD) consisted of undertaking; the production of additional documentation, software analysis and testing, plus making a claim on focussed operating experience for the firmware where this was judged to be possible. These activities align with the compensatory measures required by HSE SAP ESS.27 to address gaps in a production excellence demonstration.

108 The Software Modifications, including those to the ABB Master Programming Language Configuration Control (ACC) Advanced Application builder tool software, removed defects in order to create the nuclear software baseline AC 160 V1.3. The modifications were undertaken in compliance with good practice (i.e. IEC 60880:1986 and its supplement).

109 The Design Restrictions placed on the platform software and hardware included administrative steps to prevent the use of:

- some Programmable Control elements (e.g. element BGET that reads one bit from and element BSET that writes one bit to memory);
- the AF100 bus coupler as bus master; and
- options like event handling.

Use of these restricted items would potentially threaten the correct operation of the platform.

110 The Additional Steps included a CCF evaluation, static analysis of the critical code, modules' tests, and an integrated system test. The CCF evaluation addressed the potential for CCF initiation by interactions: within the AC 160 system and with external sources (e.g. inputs and operator demands). The static analysis covered all partitions irrespective of their SCI and included, for example, demonstration of compliance with IEC 60880:1986 (Ref. 59). Separate evaluations of the AC 160 hardware, its environmental qualification and the tools supporting the generation of application software were completed. The process was subject to oversight by a utility and external scrutiny, principally by a TuV organisation.

111 The Oskarshamn work was summarised in the Final Quality Assessment and Justification (FQAJ) Report (Ref. 61) that concluded the base software AC 160 1.3/0 and the ACC tool Advanced 1.7 are suitable for Class 1 SIS use.

112 The initial submission to the US NRC in 1999 consisted of a topical report and the Common Q software manual for NRC to review against their Standard Review Plan (Ref. 62). WEC provided a number of further submissions including appendices to the topical report covering; specific applications of the Common-Q platform (e.g. plant protection and

post accident monitoring), environmental qualification and the Oskarshamn DLCE and GOHE reports.

113 Following a series of iterations and report updates, NRC confirmed the Common Q could be used for digital C&I subject to a number of conditions. The submission history and US NRC responses are documented in the Common Qualified Platform Topical Report (Ref. 63).

114 In relation to the use of the AC160 platform in the implementation of Class 1 SSs, I sought to establish the adequacy of:

- the original AC 160 nuclear baseline (i.e. version 1.3/0);
- the development and progression to the current nuclear version (i.e. AC 160 1.3/8); and
- new components.

115 WEC provided a large amount of documentation on the AC 160 platform from the Oskarshamn 1 qualification exercise and the US NRC Common Q platform review. The review of the information against the HSE SAPs and IEC standards identified that the WEC documents, supporting SCMs and clause-by-clause analysis lacked the necessary detail. In particular, there was no clear identification of the arguments and supporting evidence used to substantiate claims made for the platform.

116 Consequently, I arranged a series of technical meetings to facilitate review of the development processes and platform substantiation from the Oskarshamn exercise. I used topic related TQs and a checklist to set the meeting expectations. The checklist (Ref. 64) outlined my expectations for the evidence needed to substantiate the adequacy of the AC 160's Programmable Complex Electronic Components (PCECs). The PCEC checklist used relevant HSE SAPs, published and draft IEC standards as the basis for its guidance.

117 The meetings aided my understanding and provided access to proprietary AC 160 documents that were only available for review in ABB offices. WEC generated additional documentation including:

- a Product Specification (Ref. 65) describing the application of the AC 160 platform to the AP1000 reactor protection role;
- an addendum to the FQAJ (Ref. 66) that provides a roadmap to the Oskarshamn documentation; and
- a "deviation" matrix (Ref. 95) to document compensating measures for areas of non-compliance with current good practice (e.g. as represented by IEC standards).

118 As a result of the identified concerns on the adequacy of the safety case documentation, I raised RO-AP1000-101 (Ref. 43) seeking a BSC for the PMS and its AC 160 platform (see Section 4.1.1). The RO gave guidance on the expected content of the BSC.

119 The AQD made use of both general platform and focussed operating history data to support the safety case. However, the safety case did not provide information on the data collection processes. Therefore, further justification is required on the robustness of the data collection processes and the appropriateness of the use of the data to support a proven-in-use argument.

120 The AQD made use of testing at software component, module and integrated system level. The purpose of the different tests and the way they provide compensatory evidence to support the safety demonstration requires clarification. The test data sets

have a number of sources including; test sets used for commercial development of the AC 160, and test sets derived from source code and user documentation reviews. The suitability of the test sets and the test coverage they provide requires further justification.

121 The scope of the software subjected to static analysis requires explanation and justification in respect of software module coverage and rigour of analyses. The objective of the different types of analysis (e.g. compliance with IEC 60880 and static analysis) undertaken requires clarification in terms of its adequacy and contribution to the compensatory measures.

> *GDA Assessment Finding: **AF-AP1000-CI-009** – The Licensee shall produce a comprehensive demonstration that the Added Quality Demonstration compensatory measures (i.e. the use of operating history, testing and static analysis) have adequately addressed the gaps identified during the qualification exercise for the original development of the AC 160 version 1.3/0. For further guidance see T15.TO1.03, T15.TO2.01 a, b and c, T15.TO2.03, T15.TO2.07, T15.TO2.08, T15.TO2.32, and T15.TO2.39 b and c in Annex 5.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

122 The AC 160 platform uses a number of PCECs, for example, in the interfaces to the back plane, high speed link (HSL) and AF100 bus. The correct operation of these devices is crucial to ensure delivery of the safety functions and determinism of the system. My assessment determined that the development processes used for the PCECs do not align with my expectations for a demonstration of production excellence (e.g. as judged against the expectations set down in the PCEC checklist). Compensatory measures are needed to address the production excellence gaps. A justification of the adequacy of the compensatory measures taken (e.g. as compared with the expectations in the PCEC checklist (Ref. 64)) is required. A safety demonstration will be needed for each PCEC development process.

> *GDA Assessment Finding: **AF-AP1000-CI-010** – The Licensee shall produce a safety justification for each Programmable Complex Electronic Component (PCECs) used in all Systems Important to Safety. The Licensee shall identify any deviations (i.e. gaps) from production excellence (as judged against an agreed standard) and demonstrate how the compensatory measures have adequately closed the gaps. This shall include demonstrating how test scripts were derived (e.g. from the requirements) and completion of the PCEC checklist. For further guidance see T15.TO2.01 b and d, T15.TO2.08, T15.TO2.27 and T15.TO2.39 a, b and c in Annex 5.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

123 The commercial version of the AC 160 (i.e. V1.2) was the starting point for the qualification exercise described above. The AC 160 V1.2 software was modified to create the nuclear baseline AC 160 V1.3/0. The claim made is that these changes were compliant with IEC 60880:1986 (Ref. 59) and its supplement (Ref 60). A robust demonstration of this claim (i.e. by provision of argumentation and evidence) is required including:

- identification of the process / procedures used (e.g. for configuration control and change management);

- documented demonstration of adherence to the processes and procedures;
- identification and justification of the software system build process including selection of compiler options;
- identification of the linkage of the test cases to the requirements; and
- demonstration of adequacy of test coverage.

124 WEC claim that the processes used for modifications to the nuclear baseline AC 160 V1.3/0 in order to create the current version V1.3/8 were compliant with IEC 60880. The records examined indicate that a number of process changes were made during this period.

> *GDA Assessment Finding: **AF-AP1000-CI-011** – The Licensee shall substantiate the claim of IEC 60880 compliance for the changes made to the AC 160 to create:*
>
> - *the AC 160 V1.3/0 nuclear baseline from the V1.2 software; and*
> - *each subsequent AC 160 release (i.e. versions from V1.3/0 to V1.3/8).*
>
> *The Licensee shall document the change process used to create each of the software versions referenced above and demonstrate its adequacy.*
>
> *The Licensee shall ensure the demonstration of compliance with IEC 60880 addresses all relevant clauses such as change management, configuration control, software build, verification and test. The Licensee shall demonstrate that the tests adequately addressed the modifications (e.g. the tests addressed the changes to the requirements and provided adequate code coverage). For further guidance, see T15.TO2.05, T15.TO2.06, T15.TO2.28, T15.TO2.34, T15.TO2.39 b, c and d, and T15.TO2.46 in Annex 5.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

125 The assessment identified a number of specific issues relating to the platform that require additional substantiation including; the checking of random access and other memory, the operation of the distributed interpreter, and the operation of the communications links including demonstration of determinism (e.g. response of HSL to a failure).

> *GDA Assessment Finding: **AF-AP1000-CI-012** – The Licensee shall ensure that the adequacy of random access and other memory checking is substantiated in the BSC along with the operation of the distributed interpreter and the determinism of the communication links. For further guidance see T15.TO2.43 and T15.TO2.63 a and b in Annex 5.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

126 For the AP1000 PMS application, WEC has still to complete the development and qualification of the following AC 160 components to Class 1 standards:

- pulse counter card DP620;
- analogue input cards AI687 and AI688;
- AF 100 bus including its communications cards CI631 and CI527; and

- flat panel displays.

In addition, WEC need to complete the production of a BSC for the AC 160 platform in its AP1000 PMS role.

127 I have raised GDA Issue **GI-AP1000-CI-08** in Section 4.4 for WEC to provide a BSC for the PMS. The PMS BSC should include the safety demonstration for the AC 160 platform. The guidance contained in Annex 2 (GDA Issue **GI-AP1000-CI-08** section) is applicable to the AC 160 platform safety demonstration.

128 I have completed a sample-based assessment of the PMS documentation and reviewed the information made available at meetings with WEC. As a result of my assessment, I conclude that the AC 160 platform is, in principle, able to support a Class 1 Safety System. This conclusion is subject to the satisfactory resolution of the Assessment Findings and GDA Issue **GI-AP1000-CI-08** recorded in this report.

4.3.1.2 Assessment of the CIM

129 The CIM is a key Class 1 component of the PMS as it provides the:

- interface to the equipment providing the Engineered Safety Features (ESF) functions;
- prioritisation logic to allow control of the ESF equipment by the PLS; and
- proposed interlock logic to reduce the probability of spurious operation of the primary circuit depressurisation valves.

130 The CIM consists of a module that carries out the priority logic function and the SRNC that provides the communication interface to the PMS; both elements use FPGA technology. The CIM reliability target was initially the same as the PMS. With the proposed addition of the interlock function, the CIM potentially has a higher reliability requirement that needs to be determined.

> *GDA Assessment Finding: **AF-AP1000-CI-013** - The Licensee shall determine and justify the reliability target of the Component Interface Module (CIM) in the AP1000 and demonstrate the adequacy of the CIM production processes in relation to the reliability target.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

131 Little information on the CIM development process and its implementation was available until late in GDA Step 4. WEC made this information available for a limited time (as for the AC 160) at review meetings. The BSC requested by RO-AP1000-100 (Ref. 44), and supplied in November 2010, was the prime source of information for my review.

132 I established that the supplier was new to the nuclear market. Examination of the CIM development processes and the outputs available from the CIM development showed them to be immature. The CIM is a key Class 1 component but it is complex. I identified and WEC has acknowledged (Ref. 48), that the CIM design process and supporting justification needs improvement to fully meet expectations as defined by appropriate standards and guidance (e.g. PCEC checklist).

133 The CIM design and its implementation progress in a series of steps starting from the WEC requirements' documents. The development process description in the supplier's procedures identified the process as a gated one. The gated process facilitates control of progression from step to step, and the performance of verification and validation (e.g. of

the FPGA programme development, FPGA device configuration and hardware board development).

134 The review of CIM documents identified the WEC functional requirement input documents. However, the non-functional requirements in respect of QA arrangements and standards compliance were not apparent (e.g. for defensive design). The functional requirements were not consistently tracked from one step to the next in the development. For some requirements the tracking was lost at the very first step (see T15.TO2.10 b and c, T15.TO2.15 a, and T15.TO2.42 a and b in Annex 5).

135 The application of the gated process was not apparent from the development records made available for review. Evidence to confirm the rigorous application of configuration control could not be identified (e.g. the configuration baseline for the design products at the end of each step). The apparent lack of configuration control revealed by the documentation review is consistent with the lack of evidence of adequate change management.

136 Review of the development process documentation identified the use of testing and simulation as important contributors to the demonstration of a rigorous development process. However, my review revealed that further clarity is needed on the configuration status of the:

- equipment under test (i.e. FPGA programme code, FPGA or board);
- the test equipment;
- output from the simulation activities (e.g. following: generation of the HDL, synthesis, and place and route).

The source of the test scripts was also unclear.

137 The apparent lack of application of the gated process and 'freeze' points was also evident in respect of the verification and validation (V&V) processes. For example, I could not identify the development process verification points from the document set presented for review. This is consistent with the observation that I could not identify the document sets used for the CIM 'design' reviews (see T15.TO1.10c, d and g, T15.TO2.10c, T15.TO2.11, T15.TO2.12 and T15.TO2.42c in Annex 5).

138 Good practice for Class 1 system development requires the independence of staff undertaking design, test and V&V activities. This requirement for independence is contained in the PCEC checklist and it is derived from the requirements of IEC standards including BS IEC 61513 and BS IEC 60880. I have included reference to BS IEC 60880 since FPGA application logic development shares many features with software development. The supplier had undertaken an independent V&V exercise but the verification revealed that the inputs were poorly defined as no configuration baselines could be identified. The degree of independence of personnel in respect of the other development activities including the design and test activities was not apparent (see T15.TO1.10b and T15.TO2.11 in Annex 5).

139 The observations above challenge any claim of production excellence for the CIM development (i.e. as expected for a new component in a Class 1 Safety System using FPGA technology).

*GDA Assessment Finding: **AF-AP1000-CI-014** - The Licensee shall provide a comprehensive demonstration of the fitness for purpose of the Component Interface Module development process that addresses, amongst others: 1) requirements identification and traceability; 2) configuration management and change control; 3)*

verification and validation; and 4) staff independence. For further guidance in relation to 1) see T15.TO2.10b and c, T15.TO2.15a, and T15.TO2.42a and b; 2) see T15.TO2.16; 3) see T15.TO1.10c, d and g, T15.TO2.10c, T15.TO2.11, T15.TO2.12 and T15.TO2.42c; and 4) see T15.TO1.10b and T15.TO2.11 in Annex 5.

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

140 The CIM BSC (Ref. 48) reports the outcome of a self-assessment of the development process completed by WEC. This identified five areas for improvement in relation to the suppliers' development activities covering:

- design documentation;
- requirements traceability;
- test process;
- configuration management; and
- independent verification and validation.

My assessment had identified the above areas as concerns. WEC is undertaking a major programme of compensating measures to address the identified areas for improvement.

*GDA Assessment Finding: **AF-AP1000-CI-015 -** The Licensee shall: 1) document in detail the areas for improvement established in WEC's self-assessment of the Component Interface Module development; 2) confirm the adequacy of the WEC assessment; and 3) demonstrate that the programme of compensatory measures has successfully addressed the areas for improvement.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

141 WEC has stated, in the BSC (Ref. 48), that it is to undertake its own independent testing as part of the WEC IV&V exercise. This is in accordance with the recommendations for Class 1 systems' development as defined in BS IEC 61513 and the HSE SAPs (Refs 10 and 4). WEC do not address the adequacy of the IV&V approach in detail in the BSC. WEC state that the IV&V will include simulation and testing of the hardware description language (HDL) and FPGAs using diverse tools and test vectors to those used in the development. Additionally document reviews will be performed.

*GDA Assessment Finding: **AF-AP1000-CI-016** - The Licensee shall demonstrate that an adequate independent verification and validation exercise has been applied to the Component Interface Module (e.g. by comparison with good practice represented by IEC standards). The demonstration should highlight the diverse nature of the exercise including use of diverse tools, simulations and test vectors.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

142 The US NRC has also examined the design processes used by the supplier in the context of the development of the CIM for use in safety systems and a controller for a non-safety application. The US NRC report includes a number of findings (Ref. 67), in respect of the supplier's processes that need to be addressed by the supplier.

*GDA Assessment Finding: **AF-AP1000-CI-017** - The Licensee shall ensure that the non-compliances raised by the US NRC (Ref. 67) in respect of the Component Interface Module development have been resolved to the Licensee's satisfaction.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

143 The development process for the CIM makes use of complex software based development tools to host the processes and check the outputs. The tools, their role in the development process and contribution to safety need to be defined. For example, there should be a demonstration of the adequacy of the Automatic Test Environment tool used for Class 1 Safety System development. There should also be evidence of configuration control of the tools once they have been justified as suitable.

*GDA Assessment Finding: **AF-AP1000-CI-018** - The Licensee shall ensure: the role of the complex software tools used to support the Component Interface Module development (e.g. for production of the Field Programmable Gate Array's Hardware Description and for testing) is identified; the tools have been justified as suitable for Class 1 development; and the tools are placed under configuration control. For further guidance see T15.TO1.10 e and f in Annex 5.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

144 The CIM BSC describes a number of diagnostic and self-test features of the CIM and SRNC including the dual core design, built in self-testing, output testing, and safety path overlap testing. The descriptions are not clear on the actual coverage of the tests (e.g. functional and of check features), the failures they detect, or the response in the event that an error / failure is detected. The effectiveness of this testing should be clear if it is to be used to support a high reliability claim for the CIM.

*GDA Assessment Finding: **AF-AP1000-CI-019** - The Licensee shall substantiate the adequacy of coverage of the diagnostics and self-test features of the Component Interface Module. For further guidance see T15.TO1.06 b) and T15.TO2.62 in Annex 5.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

145 WEC was required under RO-AP1000-100 to provide a BSC for the CIM. The RO set out the expected content of the CIM BSC. My assessment of the BSC (Ref. 48) has identified a number of key areas for improvement, namely:

- demonstration that the development process is compliant or equivalent to IEC standards (e.g. through use of the PCEC checklist), and
- identification of the evidence to support the demonstration.

The BSC should document the standards compliance and address the issues identified above that relate to use of tools and test coverage. I have raised a GDA Issue seeking a BSC for the CIM. The rigour of the safety demonstration provided in the BSC should reflect the reliability claim on the CIM.

*GDA Issue: **GI-AP1000-CI-09** - Component Interface Module (CIM) adequacy of safety case. I have identified shortfalls in the CIM safety case (e.g. in the provision*

of a claims-argument-evidence structure). WEC need to respond to the following two actions.

- ***GI-AP1000-CI-09.A1****: WEC to facilitate ND access in the UK to the detailed evidence used to support the basis of safety case for the CIM.*
- ***GI-AP1000-CI-09.A2****: WEC to provide the basis of safety case for the completed design of the CIM that takes into account the expectations expressed in Annex 2, the CIM's reliability requirement, and the remedial action including IV&V undertaken by WEC.*

For further guidance see Annex 2, and T15.TO1.05, T15.TO1.06, T15.TO1.07, T15.TO1.08, T15.TO1.10 and their associated TO2s in Annex 5.

4.3.1.3 Assessment of the 7300 Series Platform

146 WEC changed the DAS platform from an FPGA based product to WEC's 7300 series equipment during GDA Step 4. The change in platform arose from concerns that I raised on the diversity of the FPGA based DAS and CIM. The DAS and CIM were to:

- be provided by the same supplier;
- be developed using the same processes and tool sets; and
- use FPGAs supplied by the same FPGA vendor.

For further discussion on this topic see Section 4.6.

147 I sought a BSC for the DAS (Ref. 45) following the change of its platform and architecture. WEC responded by providing a DAS BSC (Ref. 50) that includes a very detailed description of the DAS design concept, its assembly from the 7300 series cards and its mode of operation as a system.

148 The BSC identifies the set of DAS boards. The boards use analogue / discrete digital technology of defined functionality. The boards were developed for control and protection applications. They have been used extensively in a wide range of WEC nuclear plant. This has included use in systems performing a role equivalent to those of UK Class 1 protection systems.

149 The BSC lacked board development and change management process details (i.e. as applied from board inception to date). The 7300 series equipment development processes predate those expected by current standards. WEC did not put forward an argument as to the adequacy of these processes (see T15.TO2.14, T15.TO2.16, T15.TO2.18 and T15.TO2.53 in Annex 5).

150 The BSC claims a demonstration of adequacy of the boards by an argument of proven-in-use both directly, and indirectly by reference to operational experience data. However, no substantive evidence of the operating history was presented to support the claims (see T15.TO2.21 in Annex 5).

*GDA Assessment Finding: **AF-AP1000-CI-020** - The Licensee shall ensure that: i) the DAS BSC justifies the adequacy of the development processes used for the 7300 series boards used in the DAS application and ii) claims of proven-in-use / reliance on operating history are made explicit in the BSC. For further guidance see T15.TO2.14, T15.TO2.16, T15.TO2.21 and T15.TO2.53 in Annex 5.*

[Time: Prior to nuclear island safety related concrete.]

151 The BSC addressed the reliability of the DAS platform. However, it did not provide detail of the design and analysis work undertaken to support the reliability claims for the boards. In addition, it did not explain the steps taken to demonstrate that the boards have known / preferred failure modes.

> *GDA Assessment Finding: **AF-AP1000-CI-021** - The Licensee shall ensure that the analysis of the 7300 board failure modes and reliability is completed and documented as part of the DAS platform substantiation. For further guidance see T15.TO2.24, T15.TO2.25 and T15.TO2.26 in Annex 5.*
>
> [Time: Prior to nuclear island safety related concrete.]

152 I have concluded that the history of the 7300 platform is such that, in principle, it should meet the DAS platform requirements. However, WEC has not provided the supporting evidence such as that required to make a proven-in-use argument.

153 I have raised GDA Issue **GI-AP1000-CI-01** in Section 4.4 that addresses the need for WEC to introduce formally the DAS design changes and provide a DAS BSC. The DAS BSC should include the safety demonstration for the 7300 series platform. The guidance contained in Annex 2 (**GI-AP1000-CI-01.A2** section) is applicable to the 7300 series platform's safety demonstration.

4.3.1.4 Assessment of the Ovation Platform

154 The Ovation platform was originally developed by WEC for plant automation applications including those of nuclear facilities. Emerson has undertaken the platform development over the last decade, working to commercial rather than nuclear specific standards. My initial assessment revealed that there was very little detailed documentary evidence available for review.

155 In the absence of detailed documentation, the assessment was progressed by raising TQs that requested further information and at a meeting where WEC presented the Ovation platform capability and components. WEC also outlined the development processes that it proposes for the PLS / DDS applications that are to be implemented using the Ovation platform. A request for more detailed information to be made available was formalised in RO-AP1000-78 (Ref. 41). RO 78 sought an explanation of how:

- WEC assured itself that the Ovation platform is fit for use in Class 2 and 3 SIS;
- the Ovation development and maintenance processes conform to HSE SAPs ESS.27, ESR.5 and ESR.4; and
- WEC validate the correctness of the Ovation configuration performed by the supplier.

156 The WEC response (Ref. 46) to RO-AP1000-78 addresses the areas above in turn. In each area a set of topics was identified (e.g. Quality Control of the procurement of Commercial-Off-The-Shelf (COTS) equipment). The submission made a series of claims and identified the supporting evidence. An example of a claim made is that the procurement of the AP1000 PLS and DDS Ovation based equipment is controlled appropriately in relation to its equipment classification.

157 The basis of the WEC approach, including the source of the topics and claims or reason for their selection is not identified or immediately apparent. For example, the topics and claims do not appear to be linked to standards' requirements. While the topics and claims appear to be appropriate, the safety argument that they support is not apparent. The supporting evidence is often presented as an assertion without identification of

convincing documentary evidence. For example, for evidence in one case WEC has simply stated, "WEC has reviewed the Emerson Process Management Power & Water Solutions, Inc. Quality Management System Manual and supporting product development procedure and found them to be appropriate for Commercial Off The Shelf (COTS) process control equipment". The evidence presented in this case identifies neither the standards nor the requirements against which the review was undertaken. In addition, there is no reference to the documented review output.

> *GDA Assessment Finding: **AF-AP1000-CI-022** - The Licensee shall ensure that the Ovation platform claims identified in the response to RO 78 (Ref. 46) provide a complete safety argument. The Licensee shall identify the evidence supporting the claims by reference to documents that substantiate the claims. The Licensee shall ensure that the claims-arguments-evidence trail is presented in or referenced from the PCSR / safety case.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

158 I have raised a GDA issue seeking a BSC for the Ovation platform to justify its use in Class 2 and 3 SIS.

> *GDA Issue: **GI-AP1000-CI-06**: Ovation platform adequacy of safety case. WEC to provide an adequate safety case for the Ovation platform that supports the Class 2 closed loop controls and the Class 3 manual controls and displays of AP1000. WEC need to respond to the following two actions.*
>
> - ***GI-AP1000-CI-06.A1**: WEC to facilitate ND access in the UK to the detailed evidence used to support the basis of safety case for the Ovation platform.*
> - ***GI-AP1000-CI-06.A2**: WEC to provide a basis of safety case that includes a justification of the suitability of the Ovation platform for Class 2 and 3 SIS. The development of the basis of safety case shall take into account the expectations expressed in Annex 2.*
>
> *For further guidance on this GDA Issue see Annex 2 and T15.TO1.01 in Annex 5.*

4.3.1.5 Assessment of Pre-Developed Equipment

159 WEC's intention to make use of smart devices (i.e. devices containing computer technology) in C&I SIS was identified during GDA Step 2 (Ref. 24). In GDA Step 3 WEC confirmed that the use of smart devices would be restricted to their use in the implementation of Class 2 and 3 C&I SIS (Ref. 32). Subsequently it was established that they might be used in other SIS at Class 1 (e.g. to perform a protection role within electrical systems). However, it was apparent that WEC did not have an established process for selection and justification of smart devices used in SIS.

160 I raised RO-AP1000-70 (Ref. 68) requesting WEC to:

- state the approach to be used for the selection and use of smart devices;
- identify the process to be used for justification of the use of smart devices in Class 1, 2 and 3 SIS; and
- provide examples of the application of their justification process.

161 I prepared a check list for the assessment of smart sensors and actuators (Ref. 69) using guidance contained in relevant HSE SAPs, IEC standards and the 'Seven Parties nuclear regulators' document' (Ref. 5). I supplied the checklist to WEC for guidance and completion following selection and qualification of the example devices.

162 WEC responded to RO-AP1000-70 (Ref. 70) indicating potential smart device applications, selection criteria and an outline justification plan. WEC confirmed the approach to justification in a further response (Ref. 71). I assessed the submissions and found that the approach they outlined is acceptable, in principle, aligning with current good practice and the output from research in the UK. WEC did not provide the detailed procedures supporting the justification process and the demonstrations requested of their application. However, WEC identified the procedures and committed to supply examples demonstrating the application of the process at a future date.

163 I had planned to perform an assessment of WEC's arrangements covering the processes for qualification and use of smart devices, and to review the evidence generated by application of the processes to a selected sample of smart devices during GDA Step 4. In the absence of the detailed evidence, I have raised the following GDA Issue for provision of the procedures and examples of their application. The response to the GDA Issue should include the provision of completed smart sensor and actuators checklists (Ref. 69).

> *GDA Issue:* ***GI-AP1000-CI-05*** *- Smart device justification for use. WEC's approach to SMART devices (i.e. ones containing programmable elements) was not adequately developed. WEC need to respond to the following two actions.*
>
> - ***GI-AP1000-CI-05.A1****: WEC to provide copies of the procedures (UKP-GW-J0Y-002, 004 and 005, Refs 99 to 101) supporting the smart devices' justification process (UKP-GW-GLR-017 Revision 0, Ref. 102) for review.*
> - ***GI-AP1000-CI-05.A2****: WEC to provide the evidence from implementation of their smart devices justification process as applied to sample devices agreed with ND from the three safety classes (one for each class). This is to include the output from implementation of the WEC qualification procedures and completed smart sensor and actuators checklists (FN-C 37194/36490R, Ref. 69).*
>
> *For further guidance on this GDA Issue see Annex 2 and T15.TO2.29 in Annex 5.*

164 The GDA scope for sensors was limited to the IIS but excluded specific elements of the lifecycle (e.g. process outputs for design, implementation and test - see Section 2.3.5). The ex-core and process sensors were not included within the GDA scope. During GDA Step 4 a review of key safety case documentation for the IIS was undertaken (see Annex 3). In particular, the review considered the degree of compliance to relevant IEC standards. The review could only determine a low level of compliance for the one key standard selected for sample review.

165 In response to a TQ requesting further information on IEC standards compliance and other sensor information, WEC has stated that equivalence of the sensor standards imposed on vendors can be provided once an AP1000 contract is in place (Ref. 72). As a result, the evidence provided during GDA Step 4 did not allow the assessment against relevant IEC instrumentation standards to be completed. The Licensee will need to ensure there is an adequate safety case for such instrumentation (including demonstration of compliance to appropriate standards).

*GDA Assessment Finding: **AF-AP1000-CI-023** - Adequacy of Sensors - The Licensee shall ensure there is an adequate safety case for in-core instrumentation sensors and other sensors used in Systems Important to Safety. This shall include a demonstration of conformance to relevant IEC standards. For further guidance see T13.TO2.46 in Annex 3.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

4.3.2 Findings

166 The GDA Issues and Assessment Findings recorded in the Section above are listed in Annex 1 and 2 respectively.

4.4 C&I Systems Important to Safety

4.4.1 Assessment

167 This Section describes the outcome of my assessment of the C&I SIS (i.e. PMS, DAS and PLS / DDS) including conformance with the HSE SAPs and IEC standards. This Section complements and builds upon Sections 4.2 and 4.3 of the report. Progress with resolution of the GDA Step 3 observations (i.e. design completion, fail safety and independent confidence building) is reported below.

168 The work of the C&I TSC supported my assessment. The TSC's report (Ref. 73) describes the scope of work performed by the TSC, and the TOs arising from the work. (Ref. 73). Annex 6 provides a summary of the TSC's report (Ref. 73) including details of the TOs raised.

169 I used the contribution of the major C&I SIS to plant risk reduction as the basis for the assessment sample. The sample included the primary and secondary protection systems (PMS and DAS respectively), the major automatic plant control system (PLS), and the major manual controls and displays (DDS and OCS). These are the main AP1000 Class 1, 2 and 3 C&I SIS.

170 My SIS assessment covered the development processes and system design requirements. WEC stated that the design and implementation detail was out of scope (see Section 2.3.5). The DAS BSC presents the DAS as a design concept (Ref. 50).

171 My assessment also specifically addressed matters identified in GDA Step 3, namely:

- the incomplete nature of the design;
- failure to safety as applied to the C&I SIS (e.g. for functions that do not have an immediately recognised / unique safe state); and
- clarification of the production excellence and independent confidence building to be applied to CBSIS.

I have progressed resolution of all three items but they remain open. Their resolution is being progressed by a combination of GDA Issues (e.g. design completion **GI-AP1000-CI-01**) and Assessment Findings (e.g. independent confidence building **AF-AP1000-CI-30**).

172 My assessment of the SIS encountered similar problems to that for the platforms. In particular, the PCSR (Ref. 22), the principal safety document, makes a series of claims in respect of the C&I systems but presents little supporting argument or evidence. WEC

provided the detailed information on the SIS in the EDCD (Ref. 27) and its subordinate references. The information presented concentrates on a description of the SIS, what they do and how they do it. The information on processes and their substantiation was restricted to descriptions and documentation demonstrating compliance with IEEE standards produced in support of submissions to the US NRC.

173 I reviewed WEC's safety justification provided in its submissions including the HSE SAP compliance SCMs and the IEC standards' clause-by-clause compliance demonstration. I found that the submissions did not provide an adequate basis for assessment of the SIS. I requested that WEC supply BSCs for the SIS selected for review (see Section 4.1). The four BSCs (covering the PLS / DDS, PMS, CIM and DAS) supplied by WEC (Refs 47 to 50) formed a significant element of my assessment of the sampled SIS.

4.4.1.1 Assessment of the PMS

174 The PMS is the AP1000's "primary" protection system providing automatic reactor trip and actuation of the ESFs. The PMS also permits some manual actuations of the ESFs and the application of blocks and resets. The safety panels in the MCR and non-safety panels in the Remote Shutdown Room (RSR) provide the operator interface for these manual actuations. The PMS is a Class 1 four Division system based on the ABB AC160 platform (see Section 4.3). The PMS is a Class 1 Safety System and has a reliability claim of 10^{-3} probability of failure on demand (pfd).

175 The PMS processes the sensor inputs and determines partial trip status in the dual redundant Bistable Processor Logic (BPL) units within a Division. The partial trip states are exchanged between Divisions on unidirectional communications links and processed (using a 2-out-of-4 vote (2oo4)) in the Local Coincidence Logic (LCL) units within each Division. The final reactor trip demand to the reactor safety / control rods is also voted using 2oo4 logic in the electrical circuit breaker and motor generator control circuits. The demands for ESF action are processed further in the Integrated Logic Processor (ILP) units to determine the response required of the field devices that are initiated from the CIMs.

176 The field device (e.g. valve actuators and motor / pump control equipment) action is determined in the ILP. At this point, the 4 fold Divisional redundancy is lost and control of the individual field devices is distributed among the four Divisions. The ILPs are dual redundant within a Division. Each ILP actuates the field devices through individual CIMS. The potential spurious or inappropriate actuation of some field components (i.e. the SQUIB valves) can have onerous consequences. Either of two Divisions can actuate such components.

177 The dual redundant nature of the Divisions (e.g. the BPL and LCL) enhances system reliability. In principle, this allows completion of many maintenance and testing activities without the need to remove a Division from service.

178 The four fold 2oo4 voted divisional architecture with dual redundancy within the Divisions is an effective approach consistent with current good practice for protection systems on modern nuclear stations. Should it be necessary to withdraw a Division from service, a veto is applied and the remaining three Divisions revert to 2oo3 voting logic. The arrangement is also resilient to equipment failure within a Division. Should a Division be lost (e.g. because of equipment failure within a Division) the voting logic of the other three Divisions becomes 1oo3. The application of a veto to stop the trip demand from the failed Division changes the voting logic to 2oo3.

179 The fact that the four Divisions are not identical needs to be taken into account in a systematic manner when justifying the capability of the system in the event of loss of a Division through failure or maintenance. The Divisional differences will need to be addressed during the design and implementation of statistical testing. Statistical testing forms part of the Independent Confidence Building Measures (ICBM) for the PMS (see TSC observations T15.TO2.02 in Annex 5, and T16.TO2.07 and T16.TO1.02 in Annex 6).

> *GDA Assessment Finding: **AF-AP1000-CI-024** – The Licensee shall demonstrate that the differences of functional coverage across the PMS Divisions do not give rise to any safety concerns (such as an inability to meet the reliability requirements or the single failure functional criterion requirements) when failures occur within a Division, or any Division is taken out of service for maintenance. For further guidance see T16.TO2.07 in Annex 6.*
>
> [Time: Prior to nuclear island safety related concrete.]

180 WEC demonstrated the adequacy of its PMS application development process by completing clause-by-clause standards compliance matrices. Matrices were completed for BS IEC 61513 (Ref. 10), BS IEC 60880 (Ref. 17) and BS IEC 60987 (Ref. 18). The content of the matrices was variable in terms of both clause coverage and evidence detail, this had a significant impact on my assessment.

181 The clause-by-clause compliance matrix provided for IEC 61513 (Ref. 10) often identified several whole documents against specific clauses. In some cases the identified documents were about the development process and other documents were about the products of the process. In the former case, the scope of the document was far greater than the scope of the clause. In the latter case, what the identified document demonstrated was not always apparent.

182 The clause-by-clause analysis matrix provided for the BS IEC 60880 (Ref. 17) standard was significantly better than that for BS IEC 61513 (Ref. 10). The references in the matrix, in the majority of cases, identified the relevant document sections thereby facilitating a detailed review. My assessment confirmed that the identified evidence demonstrated compliance of the WEC development processes with many of the significant clauses of the standard.

183 The clause-by-clause compliance analysis matrix provided for the BS IEC 60987 (Ref. 18) standard had similar characteristics to those provided for BS IEC 61513 and BS IEC 60880. The mixing of evidence for the PMS and PLS / DDS was a cause of confusion. However, the detail provided was such that the identified evidence demonstrated compliance of the process with the requirements of some of the clauses.

184 An Assessment Finding in Section 4.2 covers the concerns identified above in relation to the adequacy of the standards compliance demonstration (i.e. **AF-AP1000-CI-005**).

185 I sought evidence of compliance with IEC nuclear sector C&I standards for the PMS by undertaking a deep slice review of the detailed evidence related to the PM646 controller card. A “deviation” matrix was created (Ref. 95) to record the results of the review and identify the proposed compensating measures (e.g. for areas of non-compliance to IEC standards). This evidence trail is not complete nor is it identified as part of the safety case.

> *GDA Assessment Finding: **AF-AP1000-CI-025** – The Licensee shall complete the compensating measures identified in the “deviation” matrix (Ref. 95) for the PMS and its platform, and include the matrix as evidence of compliance with good*

practice (e.g. as defined in IEC nuclear sector C&I standards) in the BSC. For further guidance see also T16.TO2.02 in Annex 6.

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

186 My assessment of the PMS has identified the need for justifications of the:

- adequacy of communication links;
- inputs to the Class 1 PMS from the non Class 1 manual panels in the RSR; and
- adequacy of control transfer arrangements from the MCR to the RSR.

*GDA Assessment Finding: **AF-AP1000-CI-026** - The Licensee shall demonstrate that the AF 100 bus and the associated communications equipment complies with Category A / Class 1 requirements, the communication response times are deterministic, and network traffic worst case loadings do not frustrate correct operation of the communications links. For further guidance see T16.TO2.09 in Annex 6.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

*GDA Assessment Finding: **AF-AP1000-CI-027** - The Licensee shall justify the acceptability of non-Class 1 inputs to the PMS from the non-Class 1 manual panels in the Remote Shutdown Room. For further guidance see T17.TO1.02b in Annex 7.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

*GDA Assessment Finding: **AF-AP1000-CI-028** - The Licensee shall demonstrate the adequacy of the means of transferring control, and the safety functions, from the Main Control Room to the Remote Shutdown Room. This shall include demonstrating the arrangements meet the requirements of the SAPs EDR.4 (single failure proof) and ELO.2 (access to SIS); and similarly for transfer of control from the Main Control Room to any other remote or local control stations.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

187 The assessment work reported under Section 4.1, covering demonstration of conformance to HSE SAPs, identified a number of HSE SAPs relevant to the PMS. A common feature of the SCMs was that it was difficult to follow the CAE trail set out in these documents. One particular difficulty was associating the precise evidence with the claims. My assessment has identified areas where further evidence is required in order to provide an adequate CAE trail (see Annex 6 for examples) as shown below.

- EDR.1 (failure to safety) - The failure modes of the PMS and particularly those parts delivering the engineered safety features are not fully defined. In addition, the means by which WEC established the preferred failure states following detection of equipment failures is not fully described (i.e. the GDA Step 3 observation remains open).
- EDR.2 (redundancy, diversity and segregation) - WEC has stated that the PMS is broadly four fold redundant. This statement does not adequately describe the internal

redundancies of the Divisions. In addition, it does not address the shortfall in four-fold redundancy across the Divisions. This prevents a full assessment of the system, as it is not apparent what the claims are, for example, in respect of periodic testing.

- ESS.21 (reliability, fault revealing) - The arguments in respect of complexity are judged to be inadequate. For example, WEC claim that HSE SAP paragraph 355, which addresses complex hardware, does not apply to the CIM, this is clearly not the case. The submission does not identify the PMS fault revealing mechanisms nor demonstrate adequate PMS fault detection coverage. The SCM suggests that periodic testing will be a significant means of fault detection. Further clarity on the adequacy of the fault revealing arrangements is needed.
- ESS.27 (CBSIS) - The PMS BSC presents an argument of production excellence for the application software development. The SCMs address compensatory measures but it is unclear how the production excellence arguments presented in the BSC and compensatory measures identified in the SCMs are aligned. The ICBMs for the PMS are considered separately below.

*GDA Assessment Finding: **AF-AP1000-CI-029** – The Licensee shall improve the content of the Safety Case Maps to:*

- *make clear the CAE trail for the individual platforms and applications;*
- *identify evidence by detailed references (i.e. by document section and paragraph);*
- *ensure all elements of the SAPs are addressed; and*
- *ensure the CAE trail presented in the SCMs is consistent with the safety arguments in the BSCs.*

For further guidance see T16.TO1.06 in Annex 6.

[Time: Prior to nuclear island safety related concrete.]

188 WEC has confirmed it will undertake additional PMS ICBMs in order to demonstrate compliance with HSE SAP ESS.27. However, WEC has still to fully define the scope and demonstrate the adequacy of the ICBMs (i.e. as raised in the GDA Step 3 Assessment Report (Ref. 6) observation). WEC has committed to:

- conduct independent reviews of its safety case (e.g. Refs 74 and 75);
- undertake statistical testing in support of the system's reliability claim (Ref. 33 Action 22 and Ref. 76 Action 19); and
- perform static analysis of the PMS application code (Ref. 77).

189 The independent review submission (Ref. 78) does not clearly explain its contribution to the ICBMs. WEC has not fully defined the scope and expectations for both statistical testing and static analysis.

*GDA Assessment Finding: **AF-AP1000-CI-030** – The Licensee shall fully define the scope and programme for independent confidence building measures to be completed for the PMS and demonstrate that their coverage is appropriate in relation to the PMS integrity claims. For further guidance see T15.TO2.66 in Annex 5 and T16.TO1.02 in Annex 6.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

190 The PMS protection algorithms require the calculation of reactor trip and ESF actuation levels. Some calculations are 'simple' (e.g. measurement to engineering unit conversions and fluid density temperature corrections). However, others (e.g. over temperature / over power trips) require significantly more computation. In addition, some of the calculated parameters are output from the PMS to the PLS for reactor control.

191 I prepared a checklist for my assessment of WEC's implementation of calculated parameters / trips (Ref. 79). In developing the checklist, I used the guidance contained in relevant HSE SAPs and IEC standards. WEC provided completed checklists (Ref. 80) in order to demonstrate the adequacy of the calculated parameters / trips but they contained significant omissions. This is, in part, because the implementation phase of the PMS life cycle is incomplete (i.e. for the UK and other AP1000 projects). Nevertheless, a demonstration of the correctness of the calculated parameters used in the generation of ESF actuations and reactor trips is necessary (e.g. via a completed checklist and generation of supporting justification).

*GDA Assessment Finding: **AF-AP1000-CI-031** – The Licensee shall demonstrate the appropriate and correct calculation of calculated parameters, and ESF actuation and reactor trip levels. The Licensee shall ensure that appropriate criteria and guidance are used in the demonstration (e.g. by completion of the calculated trip checklist and generation of a supporting justification). For further guidance see T16.TO2.08 in Annex 6.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

*GDA Assessment Finding: **AF-AP1000-CI-032** – The Licensee shall demonstrate that the use of parameters calculated by the PMS, and used by both the PMS and PLS, cannot result in a common mode failure of the PMS and PLS (in particular where mitigation of the PLS failure would require correct operation of the PMS). For further guidance see T17.TO2.02b in Annex 7.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

192 WEC has provided development records for the AP1000 C&I SIS from other projects as evidence to support the demonstration of the adequacy of the PMS production processes. This documentation will not necessarily be the same as that for an AP1000 in the UK. For example, there may be differences because of different reliability claims on the PMS and the proposed introduction of the blocker / interlock in respect of spurious operation of the PMS.

*GDA Assessment Finding: **AF-AP1000-CI-033** – The Licensee shall produce a full set of AP1000 development records that demonstrate compliance with the development processes. This should include evidence of requirements traceability, configuration control, test planning, and review and verification records. For further guidance see T16.TO2.06 in Annex 6.*

[Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

193 WEC has produced a BSC for the PMS (Ref. 49) covering both the platform and application development in response to RO-AP1000-101. My review of the BSC has identified a number of areas for improvement including to:

- the HSE SAPs and IEC standards conformance demonstration; and
- justification of the scope and adequacy of the ICBMs.

194 The PMS safety case needs to incorporate the responses to the PMS related Assessment Findings identified in this report and to reflect PMS development progress as the design is completed. I have raised a GDA Issue to cover completion of the BSC for the PMS and the provision of access to the supporting evidence (see Section 4.3 also).

> *GDA Issue **GI-AP1000-CI-08** – PMS adequacy of safety case. Shortfalls have been identified in the PMS safety demonstration (e.g. provision of a claims - argument - evidence structure). WEC need to respond to the following two actions.*
>
> - ***GI-AP1000-CI-08.A1**: WEC to facilitate ND access in the UK to the detailed evidence (e.g. ABB documentation) used to support the basis of safety case for the PMS.*
> - ***GI-AP1000-CI-08.A2**: WEC to provide a basis of safety case for the PMS (including the AC 160 platform) that takes into account the expectations expressed in Annex 2.*
>
> *For further guidance on this GDA Issue see Annex 2, and T15.TO1.02, T15.TO1.03 T15.TO1.11 and their associated TO2s plus T15.TO2.36 and T15.TO2.43 in Annex 5, and also T16.TO1.01 and its associated TO2s, and T16.TO1.02, T16.TO2.07, T16.TO2.08, T16.TO2.09, T16.TO2.38, T16.TO2.42 and T16.TO2.45 in Annex 6.*

4.4.1.2 Assessment of the DAS

195 The DAS provides a diverse means of automatic reactor trip and actuation of the ESFs required during the early stages of a demand for safety action. The DAS also has a manual section that duplicates the automatic functions and enables manual actuation of the ESFs required in the latter stages of a demand (e.g. operation of the ADS valves). The DAS was to be based on FPGA technology with 2oo2, energise to actuate, voting logic. Section 4.6 addresses the issue of diversity between the DAS and CIM when both use FPGA technology. This Section addresses the DAS architecture and technology.

196 I raised RO-AP1000-71 (Ref. 81) during GDA Step 4 that requested a substantiation of the DAS design. The proposed 2oo2 voting logic, with the requirement for the DAS to energise its outputs in order to actuate plant equipment, does not accord with the requirements of the HSE SAPs. For example, HSE SAP ESS.23 equipment unavailability, ESS.21 reliability and EDR.1 fail safety. The original design was such that the DAS would need to be withdrawn from service for routine maintenance and repair during reactor power operation. The DAS would also be unavailable in the event of a single random hardware failure. In both of the above cases, the AP1000 would lose its "secondary" protection system.

197 WEC committed to change the DAS platform technology from FPGA to conventional electronics (i.e. in its response to RO-AP1000-81 on CIM / DAS Diversity, see Ref. 82). WEC also agreed to change the DAS architecture from 2oo2 voting to a combination of 2oo3 and 1oo2 twice voting in response to RO-AP1000-71 (Ref. 40). These changes improved the availability of the DAS and made it more fault tolerant. WEC has also

provided a number of submissions in support of these changes including the BSC for the DAS (Ref. 50).

198 I assessed the DAS architecture proposed in the concept design (Ref. 50) (i.e. for provision of the automatic functions by a combination of dual one-out-of-two (1oo2D) voting into a two-out-of-two (2oo2) vote and 2oo3 voting). I conclude that, in principle, it meets the objective sought by RO-AP1000-71 of having a DAS that would remain in service through maintenance or repair, and in the event of a single random hardware failure (e.g. of an instrument or logic channel).

199 The design changes are currently going through due process. WEC will develop the DAS in accordance with its processes and procedures. It is noted from the BSC that the design change will also include:

- modification to the DAS automatic actuation logic to introduce a trip of the reactor and turbine based on hot leg temperature measurement; and
- provision of a second manual DAS operator station (i.e. in addition to the one provided in the MCR).

These changes have affected many of WEC's submissions on the DAS and my assessment of the DAS. These changes and lack of detail in the PCSR and its supporting documents have resulted in insufficient information being available to assess the capability and independence of the sources of power for the DAS (e.g. to identify the battery backed AC supplies and the dedicated battery supplies). I have raised GDA Issue action **GI-AP1000-CI-02.A3** to secure the necessary information for the electrical assessment.

200 I have concluded that the information made available so far, does not provide a complete justification of the change to the DAS architecture and functionality. I have raised two GDA Issues seeking the submission of a safety case for the completed design and a comprehensive demonstration of the adequacy of the DAS architecture.

*GDA Issue: **GI-AP1000-CI-01** - DAS adequacy of safety case. WEC has proposed design changes to the DAS, as a result the DAS design is not complete and this has lead to the absence of safety case argumentation and evidence to substantiate the DAS design. WEC has provided an initial basis of safety case (BSC) for the DAS and my assessment has shown that this broadly aligns with my expectations. WEC need to respond to the following two actions.*

- ***GI-AP1000-CI-01.A1**: WEC to introduce formally the change to the DAS functionality and technology via its design change process (DCP).*
- ***GI-AP1000-CI-01.A2**: WEC to provide a basis of safety case for the completed design of the DAS that takes into account the expectations described in Annex 2.*

For further guidance see Annex 2, and T15.TO2.14, T15.TO2.16, T15.TO2.18 to 26 and T15.TO2.54 in Annex 5, and also T16.TO1.03 and its associated TO2s, T16.TO1.04, T16.TO2.17, and T16.TO2.43 in Annex 6.

*GDA Issue: **GI-AP1000-CI-02** - DAS adequacy of architecture. WEC has proposed significant changes to the architecture of the DAS (i.e. from a 2 channel 2oo2 voted system to a system whose logic is a combination of 2oo3 or 1oo2 twice voting). The expectation is that this modified architecture will allow the DAS to remain in service during power operation but this needs to be substantiated as the detailed design and reliability analyses are completed. The substantiation should also demonstrate*

that both the automatic and manual DAS can achieve their declared reliability targets. WEC need to respond to the following three actions.

- ***GI-AP1000-CI-02.A1****: WEC to provide a substantiation that the automatic DAS remains in service during reactor power operation including meeting the requirements for maintenance and proof testing. Note the substantiation should be included in the basis of safety case for the DAS.*
- ***GI-AP1000-CI-02.A2****: WEC to provide a substantiation that the automatic and manual DAS meet their reliability targets. Note the substantiation should be included in the basis of safety case for the DAS.*
- ***GI-AP1000-CI-02.A3****: WEC to identify and provide a description of the sources of electric power for the DAS along with their physical location on the plant.*

For further guidance see Annex 2, and T16.TO1.04 and T16.TO2.17 in Annex 6.

4.4.1.3 Assessment of the PLS / DDS

201 The PLS includes the main closed loop controls necessary for plant operation including control rod position, pressuriser pressure and level control, and steam generator level control. The DDS provides the operator controls, displays and alarms for normal plant operations. The PLS and DDS are treated as non-safety systems in the classification scheme used by WEC for the design of the AP1000. The PCSR (Ref. 22) and the EDCD (Ref. 27) were found to contain information on the functionality of the systems controlled by the PLS but little or no information on the equipment or the design and development processes. In particular, there are no references identified that are equivalent to the PMS Common Q topical report or programming manual etc.

202 I progressed this concern with WEC initially via TQs and at a meeting where WEC presented its PLS and DDS development processes. My concern that there was a significant shortfall in the provision of safety case information for the PLS and DDS was formalised in RO-AP1000-80 (Ref. 42). RO-AP1000-80 sought a demonstration of:

1) production excellence including compliance to key HSE SAPs and level 1 IEC nuclear sector;
2) the adequacy of tools; and
3) the suitability of the Personal Computers (PCs) and workstations that use commercial operating systems.

203 The WEC response was delayed (to August 2010) and then its delivery coincided with discussion on the protection systems (PMS and DAS), consequently the assessment was delayed to the end of the GDA Step 4 assessment programme.

204 The WEC response to RO-AP1000-80 (Ref. 47) addresses the three areas above in turn. In each case, WEC identified a set of topics (e.g. Quality Control of the Procurement of COTS Equipment). Then a series of claims were stated and supporting evidence identified. For example, WEC claimed that the procurement of the AP1000 PLS and DDS Ovation based equipment is controlled appropriately for the equipment classification.

205 Although the basis of WEC's approach was straightforward, the safety submission failed to meet my expectations. The source of the topics and claims was not apparent (e.g. there is no link to standards requirements). While the claims appear to be relevant, the safety argument that they support is not apparent. As for the Ovation platform, WEC

often present the evidence supporting the claims as assertions without identification of convincing documentary evidence (see Ovation example in Section 4.3).

206 The supporting evidence provided or identified in respect of the demonstration of compliance to the HSE SAPs and standards (i.e. RO-AP1000-80 item 1, see above) for the development process draws on the NuStart QA plan / programme. WEC describe its approach as being in accordance with both its QMS and system specific processes. The submission addresses how the procedures WEC has in place are self-consistent. The specific processes include configuration management, design, testing and verification. WEC do not directly address the matter of compliance with the HSE SAPs or good practice as represented by IEC standards. For example, no argument of production excellence is apparent and the compliance matrices are sparsely populated in respect of the PLS and DDS systems (see also T16.TO2.21 and T16.TO2.22 in Annex 6).

207 The response on tools (i.e. RO-AP1000-80 item 2) provides a description of the tools and their function but does not address;

- the need for them;
- the rationale for their choice;
- their role in the development process;
- how the tools are used; or
- how the tools complement one another in the interests of safety.

Evidence of adequacy of the tools is, by implication, a proven-in-use argument but this is not presented in a systematic manner (see also T16.TO2.20).

208 The discussion on the use of workstations, PCs and pre-developed equipment (i.e. RO-AP1000-80 item 3), follows the claims, argument and evidence model. WEC claim that the application of its QA arrangements and development processes ensures that the workstations, PCs and pre-developed equipment are fit for purpose. However, the claim does not address the appropriateness of the equipment itself. The argument of adequacy is based on claims of future system testing and positive experience in previous use (see also T16.TO2.23 in Annex 6).

209 Whilst these arguments are, in principle, acceptable they must be set in the context of a BSC. The arguments can form the basis of a sound safety justification. However, the gaps (e.g. in the demonstration of HSE SAPs conformance and standards compliance) need to be addressed. I have, therefore, raised a GDA Issue seeking a BSC for the development of the PLS and DDS systems.

> *GDA Issue: **GI-AP1000-CI-07** - DCIS adequacy of safety case. AP1000 automatic and manual controls, and displays are provided by the DCIS (PLS/DDS). Elements of the DCIS have to be justified as Class 2 (PLS) and Class 3 (DDS) respectively as part of the plant safety case. This requires a new justification as the systems are given a non-safety classification in the US. WEC need to respond to the following two actions.*
>
> - ***GI-AP1000-CI-07.A1**: WEC to facilitate ND access in the UK to the detailed evidence used to support the basis of safety case for the PLS and DDS applications.*
> - ***GI-AP1000-CI-07.A2:** WEC to provide a basis of safety case that includes a justification of the suitability of the PLS application at Class 2 / 3 and the DDS*

application at Class 3. The basis of safety case shall take into account the expectations described in Annex 2.

For further guidance on this GDA Issue see Annex 2, T15.TO2.36 in Annex 5, T16.TO1.05 and its associated TO2s, and T16.TO2.19 to 27 in Annex 6.

4.4.2 Findings

210 The GDA Issues and Assessment Findings recorded in the Section above are listed in Annex 1 and 2 respectively.

4.5 C&I System Level Architecture

4.5.1 Assessment

211 At the start of GDA 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 RI. One area of concern that was identified was the reliability claims on the PMS and PLS (see below). Further review of the C&I system level architecture has been undertaken during GDA Step 4. This review included consideration of WEC's responses to GDA Step 3 observations and queries raised during GDA Step 4. An important element of the GDA Step 4 work was to review the evidence presented by WEC that supports the architecture related claims and arguments (i.e. as presented in the PCSR and identified references). A summary of the outcome of the TSC's GDA Step 4 review (Ref. 83) of C&I system level architecture including TOs can be found in Annex 7.

212 The C&I system level architecture (Ref. 22) is comprised of:

- PMS (Class 1 - implemented on the AC 160 platform);
- DAS (Class 2 - implemented using WEC 7300 series equipment);
- PLS (Class 2 / 3 – implemented on the Ovation platform);
- TOS (Class 2 to meet power production requirements);
- DDS/OCS (Class 3);
- IIS (Class 1, 2 and 3 elements);
- SMS (Class 3);
- RMS (Class 1 and 3 elements);
- sensors and actuators; and
- networks.

213 The objective of the C&I system level architecture reviews was to consider the overall system architecture (C&I systems) looking at safety design features in the WEC submission, namely:

- defence-in-depth and failure mode management including CCF;
- independence and diversity;
- provision for automatic and manual safety actuation; and
- appropriateness of equipment type and class.

214 It is important that the C&I architecture is based on an overall consideration of the safety functions that have to be performed, including the category and reliability of the functions. In assigning the functions to systems, consideration should be given to the maintenance of independence. A key aspect of this is to establish that a failure in a lower safety class system cannot frustrate the correct operation of systems of a higher safety class. Another important claim that should be justified is the robustness to failure of systems involved in communication of important safety display information sent to the main control room. The rigorous definition of the overall system architecture including assignment of functions to systems, and definition of interface and independence requirements assists with the demonstration that there are no safety deficiencies in the overall system architecture.

215 The review 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 (Refs 8 and 9) and nuclear sector IEC C&I standards (e.g. Refs 10 and 11).

216 The GDA Step 3 assessment concluded that the AP1000 C&I architecture is in accordance with many of the relevant nuclear sector principles, standards and guidance documents. However, areas were identified where further clarification and substantiation was required (Ref. 6), 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);
- 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 ND's special case procedure for complex hardware);
- interconnectivity of systems on and off site; and
- segregation of C&I systems to ensure a lower safety class system cannot frustrate the correct operation of a higher safety class system.

217 My GDA Step 4 assessment has determined that the category of the safety functions and the class of the systems used to implement the safety functions is in accordance with our expectations as defined by BS IEC 61226 (Ref. 28) and BS IEC 61513 (Ref. 10) (see Section 4.2).

218 In assigning functions to systems WEC has given due consideration to the maintenance of independence of key communication links thereby satisfying the concerns on robustness to failure discussed in the previous paragraphs.

219 The interconnectivity of systems on and off site will need to be reviewed as part of the CBSIS security assessment (see Section 4.2). Specific comments on issues related to independence between systems of different safety class and interconnectivity of systems on site are made in the TSC report Ref. 83 (see summary in Annex 7). The Licensee will need to demonstrate that:

- it is acceptable for RSR non Class 1 controls to be input to the PMS (see GDA Assessment Finding **AF-AP1000-CI-027** in Section 4.4);

- the arrangements for transfer of control from the MCR to other control points are adequate (see GDA Assessment Finding **AF-AP1000-CI-028** in Section 4.4);
- the PMS calculated parameters that are transmitted to the PLS do not provide the potential for common cause failure of the PLS and PMS (see GDA Assessment Finding **AF-AP1000-CI-032** in Section 4.4);
- there is adequate segregation between systems of different class at the plant component interfaces (e.g. sensors, actuators and valves); and
- use of common input / output elements (e.g. sensors, actuators and signal conditioning equipment etc.) do not provide the potential for CCF of multiple SIS.

The Assessment Finding below covers the concerns identified in the last two bullet points.

220 The justification of SIS independence, potential for CCF, segregation and adequacy of diversity needs to be presented in the context of an overall demonstration of C&I architecture adequacy.

> *GDA Assessment Finding: **AF-AP1000-CI-034** – The Licensee shall ensure that an overall demonstration of the adequacy of the overall C&I system architecture is produced. This demonstration should cover categorisation of C&I functions, assignment of functions to C&I SIS, independence and segregation requirements, need for diversity and robustness to data communication link failures such that a failure in a lower safety class system cannot frustrate the correct operation of a higher safety class system. The demonstration shall include consideration of all SIS elements including input and output devices, and the potential for CCF of multiple SIS as a result of use of common elements (e.g. sensors, possibly smart) across SIS. For further guidance see T17.TO1.02, T17.TO2.01, T17.TO2.02 and T17.TO2.03 in Annex 7.*
>
> [Time: Prior to nuclear island safety related concrete.]

221 The original reliability claims for key C&I SIS challenged the accepted claim limits for C&I systems. WEC has undertaken a Probabilistic Safety Analysis (PSA) sensitivity study (Ref. 84) to investigate the impact on plant risk of using more modest reliability claims for the C&I systems. WEC has stated (Refs 32 and 33) that "IEC 61508" (Ref. 53) was used as guidance for the functional reliability claimed for each class of equipment. Reliability claims of 1×10^{-3} pfd, 1×10^{-2} pfd 1×10^{-1} pfd were used, for the Class 1, 2 and 3 equipment respectively, in the PSA sensitivity study. WEC's view is that the sensitivity study demonstrates that the plant risk is not unacceptable when these functional reliability claim figures are used.

> *GDA Assessment Finding: **AF-AP1000-CI-035** – The Licensee shall ensure that the safety case is updated to incorporate the PSA sensitivity study and its impact on C&I SIS reliability targets into the baseline model of the AP1000 PSA for the UK. For further guidance see T18.TO2.12 in Annex 8.*
>
> [Time: Prior to nuclear island safety related concrete.]

222 ND's PSA assessment team's review of the sensitivity of the WEC AP1000 Probabilistic Safety Analysis results to variations in the reliability claims for the AP1000 C&I systems determined that these had been done correctly for failures to operate on demand. However, the PSA assessment team's review did reveal that WEC did not address the

potential for spurious failures to lead to Initiating Events. WEC's sensitivity analyses did not address the possibility of C&I failures that could potentially cause an initiating event as well as failure of the actuation signals to the mitigation systems. This has been addressed by ND's PSA assessment team in their Risk Gap Analysis (RGA) and is reported in the PSA GDA Step 4 report (Ref. 85). The RGA has shown a measurable risk impact when increasing the frequencies of the C&I spurious actuations and explicitly accounting for the dependencies between initiating events caused by spurious PMS actuations and the mitigation systems actuated by the PMS. The RGA has also shown that the risk levels remain low and acceptable when the ADS blocking device (see below) is credited in the analysis.

223 My GDA Step 3 assessment identified the need for WEC to clarify how it analysed the adequacy of safety groups that implement Category A functions. The adequacy of protection provided by the PMS and DAS for plant faults has been considered in the ND fault studies assessment (Ref. 86). The fault studies assessment concluded that adequate functional diversity had not been demonstrated (e.g. across the PMS and DAS) and GDA Issue **GI-AP1000-FS-03** (Ref. 86) has been raised to cover this topic.

224 I considered the potential for CCF of the SIS during my GDA Step 4 assessment. Section 4.6 below addresses SIS diversity, which is one of the main defences against CCF. The PMS's four-train architecture provides defence against single random failures resulting in failure of the PMS. However, the original DAS design used a two-out-of-two architecture, which meant that a single failure of the DAS would render the DAS inoperable. WEC has proposed (Ref. 40) significant changes to the architecture of the DAS. WEC modified the 2oo2 voting arrangement and the architecture now uses either dual one-out-of-two (1oo2D) voting into a two-out-of-two (2oo2) vote or 2oo3 majority voting arrangement. The expectation is that this arrangement will allow the DAS to remain in service during power operation but this needs substantiation as the detailed design and reliability analysis are completed (see **GI-AP1000-CI-02** in Section 4.4).

225 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). I raised an issue relating to diversity of the CIM and DAS with WEC via RO-AP1000-81 (Ref. 87), see below under Section 4.6. In response, WEC has undertaken to implement the DAS using its 7300 series conventional electronic component based equipment. WEC's decision to base the DAS on the WEC 7300 series equipment has addressed the significant architectural concern related to total loss of automatic reactor protection because of CCF of the CIM and DAS (see Sections 4.3 and 4.4 for comments on the adequacy of the CIM and DAS safety cases).

226 My GDA Step 4 assessment identified the potential for spurious operation of plant components by the PMS as a significant plant safety challenge (e.g. by opening the four Stage 4 primary circuit Automatic Depressurisation System (ADS) valves). I raised this concern with WEC in RO-AP1000-82 (Ref. 88). In response (Ref. 89) WEC has undertaken a major review of all credible spurious initiation faults and has shown that these are bounded by existing design basis accident analyses, apart from spurious operation of the ADS Valves. For the ADS valves, WEC has acknowledged that such a transient would fall outside the acceptance criteria for a conservative Design Base Accident Analysis and that steps were required to reduce the initiation frequency for the spurious opening of the ADS valves as this could initiate a significant loss of coolant accident. Spurious operation of the in-containment recirculation valves would allow the in-containment refuelling water storage tank (IRWST) to drain potentially challenging both WEC's design criteria and the HSE SAPs. In the light of this WEC need to provide a

design basis safety case covering both spurious operation events for assessment as part of the fault studies review (see **GI-AP1000-CI-04** Actions A1 and A2 below).

227 WEC has proposed (Ref. 89) introducing a very simple instrumented interlock / blocker to the PMS. This will use the core make up tank level signal to provide an input to the Z port of the CIM controlling ADS actuation in order to block the actuation demand from the PMS and achieve the necessary risk reduction. WEC now need to fully engineer and justify its proposed solution. A significant element of this will be definition and justification of the CIM's reliability. I have raised a GDA Issue to address completion of the required work:

> *GDA Issue: **GI-AP1000-CI-04** - PMS Spurious Operation. The PMS has the capability to actuate any of the Engineered Safety Features (ESF) on the plant. This includes the potential to actuate spuriously the Automatic Depressurisation System (ADS) valves or the containment recirculation valves. The spurious operation of these functions has the potential to initiate safety significant transients such as a large LOCA or drainage of the in-containment refuelling water storage tank (IRWST). Westinghouse needs to provide a design basis safety case covering such spurious actuations. WEC need to respond to the following four actions.*
>
> - ***GI-AP1000-CI-04.A1**: WEC to provide a design basis safety case covering spurious PMS actuation of the ADS valves. The safety case will need to demonstrate that the ADS interlock / blocker device provides adequate protection against such faults or provide additional protection or justification as to why the position is acceptable.*
> - ***GI-AP1000-CI-04.A2**: WEC to provide a design basis safety case covering spurious operation of the containment recirculation SQUIB valves.*
> - ***GI-AP1000-CI-04.A3**: WEC to introduce formally the change to the PMS design to introduce the interlock / blocker on the ADS valves via the design change process (DCP).*
> - ***GI-AP1000-CI-04.A4**: WEC to complete the design of the interlock / blocker and substantiate it for its intended role.*
>
> *For further guidance see Annex 2 and T17.TO1.01 in Annex 7.*

228 WEC is currently in the process of planning to qualify its Safety / Qualified Data Processing System (QDPS) internal communications bus (currently the AF100 bus) to Class 1 standards. When the AF100 bus qualification is complete it will be applicable to the AP1000 and facilitate the display of high integrity information to the operator in the MCR. I sought to determine the Class 1 display and control provisions in the RSR and WEC advised that there are none (Ref. 90).

229 WEC documentation (e.g. Ref. 27) identifies that the MCR contains PMS (QDPS) Class 1 displays and controls in the safety panels, manual DAS Class 2 hardwired displays and controls, and DDS / OCS Class 3 computer based display and manual control workstations. The RSR contains a hardwired non-safety control panel connected via the PMS to the plant and a DDS / OCS Class 3 workstation. The DAS BSC indicates that DAS displays and controls, potentially Class 2, are available at an additional location. In addition, manual control is possible at the CIMs in the safety instrument rooms.

230 The regulatory expectation is that in the event of evacuation of the MCR, the alternate emergency location will allow the plant to be shutdown safely and plant safety maintained following safe shut down. As these are Category A functions, the expectation is that

Class 1 display and controls will be available to implement the required safety functions. Therefore, WEC need to provide Class 1 controls and displays at a suitable emergency location or demonstrate that it is not reasonably practicable to provide Class 1 displays and controls in the RSR or an alternative location.

*GDA Issue: **GI-AP1000-CI-10** - Provision of Class 1 displays and controls with one action.*

- ***GI-AP1000-CI-10.A1**: The regulatory expectation is that Class 1 displays and controls are provided in an emergency location independent of the MCR (the RSR). In their absence, WEC is required to either:*
  - *i) provide Class 1 displays and controls in an alternative emergency location; or*
  - *ii) provide a justification of why the current design choice (of hardwired Class 2 manual control panels and Class 3 computer based controls and displays) is acceptable against the SAPs and regulatory expectations. This should include an explanation, with a supporting justification, as to why it is not reasonably practicable to provide the Class 1 displays and controls in an alternative location.*

For further guidance see T17.TO1.02 in Annex 7.

231 In the GDA Step 3 Assessment Report I noted that with regard to defence-in-depth further clarification was 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 IAEA Safety Standard NS-R-1 (Ref. 19)). Of particular concern was that use is made of two digital platforms (i.e. ABB AC 160 and Ovation) and a FPGA based system. The PMS uses the ABB AC 160 platform, the PLS is based on the Ovation platform and the DAS was to be implemented using FPGA technology. The process for development of FPGAs has many similarities with those used for the development of software for computer-based systems. WEC's decision to change the DAS technology has addressed our major concern and I judge that the defence in depth arrangements are broadly in agreement with my expectations. For example, defence against failure of the control system PLS is provided by the PMS and DAS protection systems. The DAS provides defence against PMS failure.

232 The SIS Class, reliability claims, independence and defence-in-depth arrangements are broadly in agreement with our expectations as defined by nuclear sector guidance and standards. I conclude that the C&I architecture includes the main C&I systems and provisions that would be expected in a modern nuclear reactor but aspects related to GDA Issues and Assessment Findings require resolution to provide a more complete justification for the overall design.

4.5.2 Findings

233 The GDA Issues and Assessment Findings recorded in the Section above are listed in Annex 1 and 2 respectively.

4.6 Diversity of Systems Implementing Reactor Protection Functionality

4.6.1 Assessment

234 I have completed a review of the diversity of those systems implementing reactor protection functionality. The C&I safety systems included in the diversity review were the PMS (including CIM) and DAS. I selected these systems because they perform the AP1000 Category A protection functions.

235 The approach included consideration of various forms of diversity, including:

- equipment diversity (including diversity of platform);
- diversity of verification and validation;
- diversity of physical location (segregation);
- software diversity;
- functional / data diversity / signal diversity;
- diversity of design / development; and
- diversity of specification.

236 The work required the definition of a list of reactor-independent diversity characteristics, derived from relevant standards and guidance. I used the HSE SAPs, technical assessment guides, nuclear sector C&I standards (i.e. Refs 10 and 11), regulatory guidance (Ref. 5) and relevant research (Ref. 91) as a basis for determining the diversity characteristics.

237 The main finding of the preliminary review undertaken during GDA Step 3 (Ref. 6) on the diversity of systems implementing reactor protection functionality was that WEC appear 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:

- analysis of CCFs between the PMS and DAS;
- coverage of functional and equipment diversity;
- independence and segregation;
- maintenance and test; and
- use of diverse verification and validation.

238 I progressed closure of these findings during GDA Step 4. Annex 8 contains a summary of the TSC's review (Ref. 92) of these topics. The TSC has raised TOs to cover areas for improvement in relation to GDA Step 3 findings that have not been fully resolved during GDA Step 4. The TSC TOs provide further guidance on the steps required to address the GDA Issue and Assessment Findings recorded below.

239 As stated earlier the AP1000 design makes use of a CIM to resolve demands for component actuation from devices of different safety class (e.g. PMS and PLS). WEC decided to implement the CIM and DAS using very similar design processes and FPGA technology.

240 I consider that FPGAs (of the types proposed) are complex hardware technology and that the application development process has much in common with traditional software development. The DAS and CIM are both used in the control of major safety components, for example, some safety valves. I was concerned that, if the same

company designed the DAS and CIM, they might share many common features (e.g. use of the same type of complex programmable integrated circuit technology). The common features would introduce the risk of a common mode failure of both the DAS and CIM, which could result in a total loss of automatic reactor protection.

241 Use of FPGA technology would also make the demonstration of diversity between the computer-based systems (PMS and PLS) and the FPGA based systems (DAS and PMS / CIM) more challenging given the potential for commonality of the development processes.

242 Instead of using multi-million gate components from the same manufacturer and the same systems' designer for both the DAS and CIM, WEC is to (Ref. 82) implement the DAS using its 7300 series equipment. Many Class 1 Pressurised Water Reactor safety systems in the US successfully employ WEC's 7300 series equipment. The WEC 7300 series equipment uses very simple electronics. This modification has addressed, in principle, our major concerns on the diversity of the CIM and DAS. However, the absence of detailed design information (in particular for the DAS) has limited the depth of the diversity assessment (see Section 4.3 above).

243 Defence against failure of the control system PLS (and others such as the TOS) is provided by the PMS and DAS. The DAS provides defence against PMS failure. In order for such defences to be effective, the systems need to be independent and diverse. Once the DAS and PLS designs are complete a detailed diversity analysis will be required for the PMS and DAS, and for the PLS and DAS.

> *GDA Issue: **GI-AP1000-CI-03** - PLS, PMS (including CIM) and DAS Diversity Analysis. A detailed diversity analysis is required for the DAS against the PLS/DDS and the PMS. WEC need to respond to the following GDA action.*
>
> - ***GI-AP1000-CI-03.A1**: WEC to provide a detailed diversity analysis for the DAS (7300 series equipment based) against the PLS / DDS (Ovation) and the PMS (ABB AC 160). Note the analysis should be included in a basis of safety case document, for example, that for the DAS.*
>
> *For further guidance see T18.TO1.01, T18.TO2.06, T18.TO2.11, T18.TO2.19, T18.TO2.21 and T18.TO2.25 in Annex 8.*

244 Equipment diversity is used across the two computer-based platforms PMS (ABB AC 160) and PLS (Ovation). The high-level diversity information presented for the PLS and PMS show that key elements are diverse. However, WEC need to enhance the diversity analysis for these two applications and platforms to include a detailed review against appropriate diversity standards and guidance. WEC need to provide further Ovation design information to enhance the safety case for that platform (see Section 4.3) and the diversity review will need to take cognizance of this information.

> *GDA Assessment Finding: **AF-AP1000-CI-036** - PMS (ABB AC 160) and PLS (Ovation) Diversity Analysis - The Licensee shall provide a detailed diversity analysis of the PMS / PLS applications and AC 160 / Ovation platforms. For further guidance see T18.TO2.11, T18.TO2.20 and T18.TO2.24 in Annex 8.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

245 As noted above the adequacy of functional diversity across the PMS and DAS has been considered in the ND fault studies assessment (see Section 4.5).

246 Section 2.3.5 identifies a number of platforms that are out of scope. The Licensee will need to ensure that the potential for common cause failure of SIS as a result of the selection of platforms, which have common features to the already selected platforms, is addressed (e.g. TOS and PMS).

> *GDA Assessment Finding: **AF-AP1000-CI-037** - Platform Diversity – The Licensee shall, when selecting platforms for systems that are currently out of scope, review the potential for common cause failure of SIS (e.g. as a result of the use of common SIS platforms or platforms with common features). For further guidance see T18.TO2.18 in Annex 8.*
>
> [Time: prior to mechanical, electrical and C&I safety systems, structures and components delivery to site.]

247 The decision to use the WEC 7300 series equipment for the DAS has resolved, in principle, the major diversity concerns. The high-level diversity information presented for the PLS and PMS show that key elements are diverse but further substantiation is required. I conclude that, in principle, the diversity of the C&I SIS is not unacceptable but there are GDA Issues and Assessment Findings that require resolution.

4.6.2 Findings

248 The GDA Issues and Assessment Findings recorded in the Section above are listed in Annex 2 and 1 respectively.

4.7 Overseas Regulatory Interface

249 ND's generic design assessment strategy for working with overseas regulators is set out in 'Strategy for working with overseas regulators. Version 1. HSE' (Ref. 94). In accordance with this strategy, ND collaborates with overseas regulators, both bilaterally and multi-nationally.

4.7.1 Bilateral collaboration

250 ND has formal information exchange arrangements to facilitate greater international co-operation with the nuclear safety regulators in a number of key countries with civil nuclear power programmes. These include:

- the US Nuclear Regulatory Commission (NRC);
- the French L'Autorité de sûreté nucléaire (ASN); and
- the Finnish Sateilyturvakeskus (STUK).

251 During my assessment I identified concerns in relation to:

- the diversity of the CIM (in the primary protection system) and the DAS (secondary protection system) because of the use of common technology and supplier;
- the architecture of the DAS that required it to be taken out of service during power operation for test and maintenance; and
- potential for spurious operation of the PMS initiating a serious event by opening of the ADS valves.

252 Bilateral discussions were held with the US NRC on these three topics and these discussions facilitated a valuable exchange of information (e.g. provision of the US NRC CIM / DAS supplier audit report). The matters identified above were progressed by both parties, taking into account their national regulatory requirements and practices. The way in which the three concerns were resolved in the UK is discussed in Sections 4.4, 4.5 and 4.7.

4.7.2 Multilateral collaboration

253 ND collaborates through the work of the IAEA and the Organisation for Economic Co-operation and Development Nuclear Energy Agency (OECD-NEA). ND also represents the UK in the Multinational Design Evaluation Programme (MDEP) - a multinational initiative taken by national safety authorities to develop innovative approaches to leverage the resources and knowledge of the national regulatory authorities tasked with the review of new reactor power plant designs. The aim of this programme is to promote consistent nuclear safety assessment standards among different countries.

254 MDEP is expected to continue beyond GDA and ND will continue to take an active role. However, throughout the period of GDA no MDEP working group was formed on the AP1000 C&I as it required three parties to agree to set up a working group. The Chinese delegates to the AP1000 MDEP group did not see the need for a specific working group on C&I and therefore we continued the bilateral discussions with the NRC (see paragraph above).

5 CONCLUSIONS

255 This report presents the findings of the GDA Step 4 C&I assessment of the WEC AP1000 reactor.

256 To conclude, I am broadly satisfied with the claims, arguments and evidence laid down within the PCSR and supporting documentation for the C&I. I consider that from a C&I view point, the WEC AP1000 design is suitable for construction in the UK. However, this conclusion is subject to satisfactory progression and resolution of GDA Issues to be addressed during the forward programme for this reactor, and assessment of additional information that becomes available as the GDA Design Reference is supplemented with additional details on a site-by-site basis.

5.1 Key Findings from the GDA Step 4 Assessment

257 The major conclusions of my GDA Step 4 assessment are that:

- the PCSR and supporting documentation cover the main C&I SIS expected in a modern nuclear reactor;
- based on review of the standards implemented by WEC for the selected key C&I SIS and WEC's standards conformance submission, the C&I standards are broadly in accordance with those expected in the nuclear sector;
- WEC's safety cases for the PMS and DAS are in general accordance with expectations (noting that further implementation detail needs to be added to the safety cases following design completion); and
- the overall C&I architecture is generally in accordance with expectations.

258 Some of the observations identified within this report are of particular significance and will require resolution before ND would agree to the commencement of nuclear safety related construction of an AP1000 reactor in the UK. These are identified in this report as GDA Issues and are listed in Annex 2. In summary these relate to:

- changes made to the DAS architecture (i.e. from two-out-of-two actuation voting to two-out-of-three / dual one-out-of-two) to significantly improve fault tolerance and availability during plant operation;
- change of DAS technology from being based on complex Field Programmable Gate Arrays (FPGAs) to non programmable electronics in order to address a major concern on DAS and PMS / Component Interface Module (CIM) diversity;
- provision of detailed diversity analyses (PMS / DAS and PLS / DAS) which need to be undertaken as a consequence of the DAS technology change;
- provision of equipment to reduce the frequency of spurious ADS operation in the event of PMS failure;
- fully defining the approach to the justification of smart devices (based on computer technology) used in SIS and provision of a programme showing when implementation evidence will be available;
- enhancements to the safety cases for the PMS (including the AC160 platform used by the PMS), safety Class 1 CIM and the DAS;

- provision of safety cases for the safety related Class 2 / 3 DCIS (comprising the PLS and DDS and Ovation platform that fully meet expectations; and
- provision of safety Class 1 displays and controls outside of the Main Control Room.

5.1.1 Assessment Findings

259 In some areas there has been a lack of detailed information, which has limited the extent of my assessment. As a result ND will need additional information to underpin my conclusion and these are identified as Assessment Findings to be carried forward as normal regulatory business, such as standards compliance demonstration for SIS (covering the full lifecycle), and detailed analyses of the diversity between the PMS and the PLS. I conclude that the Assessment Findings listed in Annex 1 should be addressed during the forward programme of this reactor as part of normal regulatory business.

5.1.2 GDA Issues

260 I conclude that the GDA Issue(s) listed in Annex 2 must be satisfactorily addressed before Consent will be granted for the commencement of nuclear island safety related construction.

6 REFERENCES

1 *GDA Step 4 Control and Instrumentation Assessment Plan for the Westinghouse AP1000*. HSE-ND Assessment Plan AR 09/055. February 2010. TRIM Ref. 2009/463803.

2 *ND BMS. Assessment Process.* AST/001 Issue 4. HSE. April 2010. www.hse.gov.uk/foi/internalops/nsd/assessment/ast001.htm.

3 *ND BMS. Technical Reports.* AST/003 Issue 3. HSE. November 2009. www.hse.gov.uk/foi/internalops/nsd/assessment/ast003.htm.

4 *Safety Assessment Principles for Nuclear Facilities*. 2006 Edition Revision 1. HSE. January 2008. www.hse.gov.uk/nuclear/saps/saps2006.pdf.

5 *Licensing of safety critical software for nuclear reactors. Common position of seven European nuclear regulators and authorised technical support organisations*. Revision 2010. www.hse.gov.uk/nuclear/software.pdf.

6 *Step 3 Control and Instrumentation Assessment of the Westinghouse AP1000*. HSE-ND Assessment Report AR 09/037. November 2009. TRIM Ref. 2009/339207.

7 *Westinghouse AP1000 - Schedule of Technical Queries Raised during Step 4.* HSE-ND. TRIM Ref. 2010/600721.

8 *ND BMS. Technical Assessment Guide. Safety Systems*. T/AST/003 Issue 5. HSE. 10 June 2009. www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast003.htm.

9 *ND BMS. Technical Assessment Guide. Computer Based Safety Systems*. T/AST/046 Issue 2. HSE. 16 June 2008. www.hse.gov.uk/foi/internalops/nsd/tech_asst_guides/tast046.htm.

10 *BS IEC 61513:2001 Nuclear power plants. Instrumentation and control for systems important to safety. General requirements for systems*. International Electrotechnical Commission (IEC). 2001. ISBN 0 580 38154 4.

11 *BS IEC 62340:2010 Nuclear power plants. Instrumentation and control systems important to safety. Requirements for coping with common cause failure (CCF).* International Electrotechnical Commission (IEC). 2010. ISBN 978 0 580 68114 1.

12 *Software for Computer Based Systems Important to Safety in Nuclear Power Plants.* International Atomic Energy Agency (IAEA) Safety Standards Series No. NS-G-1.1. IAEA. Vienna. 2000. www-pub.iaea.org/mtcd/publications/pdf/pub1095_scr.pdf.

13 *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. ISBN 978 0 580 60524 6.

14 *The Tolerability of Risk from Nuclear Power Stations*. HSE. 1992. ISBN 0-11-886368-1. www.hse.gov.uk/nuclear/tolerability.pdf.

15 *The use of computers in safety-critical applications – Final report of the study group on the safety of operational computers.* HSC. 1998. ISBN 0 7176 1620 7. www.hse.gov.uk/nuclear/computers.pdf.

16 *Technical Guidelines for the design and construction of the next generation of nuclear pressurized water plant units*. Adopted during plenary meetings of the GPR and German experts on the 19 and 26 October 2000. www.asn.fr/index.php/content/download/15572/100931/technical_guidelines_design_construction.pdf.

17 *BS IEC 60880:2009 Nuclear power plants. Instrumentation and control systems important to safety. Software aspects for computer-based systems performing category A functions*. International Electrotechnical Commission (IEC). 2009. ISBN 978 0 580 63962 3.

18 *BS IEC 60987:2009 Nuclear power plants. Instrumentation and control important to safety. Hardware design requirements for computer-based systems*. International Electrotechnical Commission (IEC). 2007. ISBN 978 0 580 63961 6.

19 *Safety of Nuclear Power Plants: Design – Requirements.* International Atomic Energy Agency (IAEA) Safety Standards Series No. NS-R-1. IAEA. Vienna. 2000. www-pub.iaea.org/mtcd/publications/pdf/Pub1099_scr.pdf.

20 *Westinghouse AP1000 - Schedule of Regulatory Observations Raised during Step 4.* HSE-ND. June 2011. TRIM Ref. 2010/600724.

21 *Westinghouse AP1000 - Schedule of Regulatory Issues Raised during Step 4*. HSE-ND. June 2011. TRIM Ref. 2010/600725.

22 *AP1000 Pre-construction Safety Report*. UKP-GW-GL-732 Revision 2. Westinghouse Electric Company LLC. December 2009. TRIM Ref. 2011/23759.

23 *AP1000 Master Submission List*. UKP-GW-GLX-001 Revision 0. Westinghouse Electric Company LLC. April 2011. TRIM Ref. 2011/246930.

24 *Westinghouse Step 2 Control and Instrumentation Assessment*. HSE-ND Assessment Report AR 07/004. October 2007. TRIM Ref. 2007/253145.

25 *AP1000 Pre-construction Safety Report*. UKP-GW-GL-793 Revision 0. Westinghouse Electric Company LLC. March 2011. TRIM Ref. 2011/192251.

26 *Clarification of GDA out of scope items.* Letter from AP1000 Project Front Office to ND. WEC00512N. 17 February 2011. TRIM Ref. 2011/105073.

27 *AP1000 European Design Control Document*. EPS-GW-GL-700 Revision 1. Westinghouse Electric Company LLC. December 2009. TRIM Ref. 2011/81804.

28 *BS IEC 61226:2009 Nuclear power plants. Instrumentation and control systems important to safety. Classification of instrumentation and control functions*. International Electrotechnical Commission (IEC). 2009. ISBN 978 0 580 63322 5.

29 *Guidance to HSE and Environmental Agency Inspectors on the content of GDA Issues. Assessment Findings*, *Resolution Plans and GDA Issue Metrics* HSE-ND. 3 June 2011. TRIM Ref. 2011/302633.

30 *BS IEC 62138:2009 Nuclear power plants - Instrumentation and control systems important to safety* – Software aspects for computer-based systems performing category B or C functions. International Electrotechnical Commission (IEC). 2009. ISBN 978 0 580 63963 0.

31 *BSi Technical Committee NCE/8 Nuclear Power Plants - I&C Systems. A Guide to Applicable IEC Standards.* AFP – v7 – 2008_12_01. TRIM Ref. 2011/386499.

32 *C&I Step 3*. Letter from AP1000 Project Front Office to ND. WEC00087N. 28 August 2009. TRIM Ref. 2009/343656.

33 *Additional C&I Information for inclusion in the AP1000 GDA Step 4 Assessment*. Letter from AP1000 Project Front Office to ND. WEC00207N. 30 April 2010. TRIM Ref. 2010/200740.

34 *Technical information in support of Lot 2 & 3*. UKP-GW-GL-044 Revision 1. TRIM Ref. 2010/299611.

35 *AP1000 UK Safety Categorisation and Classification of Systems, Structures, and Components*. UKP-GW-GL-144 Revision 1. Westinghouse Electric Company LLC, January 2011. TRIM Ref. 2011/91066.

36 *IEC 60297-3-101. Mechanical structures for electronic equipment – Dimensions of mechanical structures of the 482.6 mm (19 in) series. Pt 3 – 101 Subracks and associated plug in units*. International Electrotechnical Commission (IEC). 2004.

37 *IEEE 1101.1-1998. IEEE Standard for Mechanical core specifications for microcomputers using IEC60603-2 connectors*. Institute of Electrical and Electronics Engineers (IEEE). 1998.

38 *IEC 60603. Connectors for frequencies below 3 MHz for use with printed boards*. International Electrotechnical Commission (IEC). 1995.

39 *AP1000 Standard Plant Metrication*. APP-GW-G1-011 Revision 3. Westinghouse Electric Company LLC. December 2010. TRIM Ref 2011/79452.

40 *Response to RO-AP1000- 71 – C&I Adequacy of the DAS Architecture. Letter from AP1000 Project Front Office to ND*. WEC 000286. 30 July 2010. TRIM Ref. 2010/344181.

41 *Notification of Regulatory Observation RO-AP1000-078 and Regulatory Observation Actions RO-AP1000-078.A1 to A4 C&I Adequacy of the Ovation Platform in AP1000*. Letter from ND to AP1000 Project Front Office. WEC70179R. 14 May 2010. TRIM Ref. 2010/216094.

42 *Notification of Regulatory Observation RO-AP1000-080 and Regulatory Observation Actions RO-AP1000-080.A1 to A3 C&I Adequacy of the DCIS (PLS & DDS) for AP1000*. Letter from ND to AP1000 Project Front Office. WEC70182R. 25 May 2010. TRIM Ref. 2010/230672.

43 *Notification of Regulatory Observation RO-AP1000-101 and Regulatory Observation Actions RO-AP1000-101.A1 and A2 PMS – Basis of the Safety Case for the AP1000 C&I.* Letter from ND to AP1000 Project Front Office. WEC70236R. 17 September 2010. TRIM Ref. 2010/431044.

44 *Notification of Regulatory Observation RO-AP1000-100 and Regulatory Observation Actions RO-AP1000-100.A1 and A2 CIM System – Basis of the Safety Case for the AP1000 C&I*. Letter from ND to AP1000 Project Front Office. WEC70235R. 17 September 2010. TRIM Ref. 2010/430640.

45 *TQ-AP1000-1031 - Nuclear Directorate request for a DAS BSC*. See Ref. 7.

46 *RO78 – Adequacy of the Ovation Platform Full Response*. Letter from AP1000 Project Front Office to ND. UN REG WEC 00358N. Westinghouse Electric Company LLC. 29 September 2010. TRIM Ref. 2010/482334.

47 *WEC AP1000 Response to RO-AP1000-080*. Letter from AP1000 Project Front Office to ND. UN REG WEC 00315N. Westinghouse Electric Company LLC. 30 August 2010. TRIM Ref. 2010/408890.

48 *Full Response to RO-AP1000-100*. Letter from AP1000 Project Front Office to ND. UN REG WEC 00416N. 2 November 2010. TRIM Ref. 2010/550995.

49 *United Kingdom AP1000 Protection and Safety Monitoring System Safety Case Basis*. UKP-PMS-GLR-001 Revision 0. Westinghouse Electric Company LLC. November 2010. TRIM Ref. 2011/82116.

50 *United Kingdom AP1000 Basis for the Safety Case of the 7300 Series Based Diverse Actuation System*. UKP-DAS-GLR-001 Revision 0. Westinghouse Electric Company LLC. November 2010. TRIM Ref. 2011/81957.

51 *C&I SAP Conformance, Safety Case Maps and CAE Trail Review for AP1000*. Tasks 11-13: FN-C 37194-36853R. Issue 1.2. 25 July 2011. TRIM Ref. 2011/420273

52 Review of C&I Systems' Classification and Standards. Task 14: FN-C 37194-36638R. Issue 1.0. 22 July 2011. TRIM Ref. 2011/420256

53 *BS EN 61508:2002. Functional Safety of electrical/electronic/programmable electronic safety-related systems*. International Electrotechnical Commission (IEC).

54 *Response to action 120 August C&I GDA Action Item Closeout Letter*. Letter from AP1000 Project Front Office to ND. UN REG WEC 000299. 20 August 2010. Westinghouse Electric Company LLC. TRIM Ref. 2010/370387.

55 *Nuclear Automation: Classification of I&C Systems*. WNA-SQ-00049-GEN Revision 1. Westinghouse Electric Company LLC. June 2010. TRIM Ref. 2011/82251.

56 *ISO IEC 27001:2005. Information technology - Security techniques - Information security management systems - Requirements. International Organisation for Standardization (IOS).* 2005.

57 *HMG 1A Standard No1 Technical Risk Assessment* - Issue 3.51. October 2009. www.cesg.gov.uk/publications/media/policy/is1_risk_assessment.pdf.

58 *Review of System Platforms and Pre-Developed Components. Task 15*: FN-C 37194-37352R. Issue 3.0. 4 August 2011. TRIM Ref. 2011/420350

59 *BS IEC 60880:1986. Software for computers in the safety systems of nuclear power stations*. International Electrotechnical Commission (IEC). 1986. ISBN 0580 368807.

60 *BS IEC 60880-2:2000. Software for Computers Important to Safety for Nuclear Power Plants. Software aspects of defence against common cause failures, use of software tools and of pre-developed software as a First Supplement to IEC Publication 880*. International Electrotechnical Commission (IEC), 2000.

61 *Oskarshamn 1 - Project O1 Mod Qualification of Category A I&C - Final Quality Assessment and Justification Report.* MOD 97-7771 Revision 6. TRIM Ref. 2011/0401604

62 *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: Standard Review Plan – 7.0 Instrumentation and Controls*. NUREG 0800. United States Nuclear Regulatory Commission (USNRC). 1996. www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0800/ch7/.

63 *Common Q Topical Report.* WCAP-16097-P-A. Revision 0. Westinghouse Electric Company LLC. May 2003. TRIM Ref. 2011/82164.

64 *HSE/NII Technical Review. Programmable Complex Electronic Components Checklist.* S.P 1440.074.013, Issue 2.2.2, 1 August 2011. Altran Praxis. TRIM Ref. 2011/406324.

65 *AP1000 PMS. AC 160 Product Specification for AP1000 PMS.* GBRA 095801 Revision C. September 2010. Westinghouse Electric Germany GmbH. TRIM Ref. 2011/76541.

66 *UK AP1000 – GDA. O1 MOD – Qualification - Final Quality Assessment and Justification Report – Addendum.* GBRA 095803 Revision B. November 2010. Westinghouse Electric Germany GmbH. TRIM Ref. 2011/0402008

67 *Audit Report for review of proprietary technical, procedural, and process information related to the component interface module and diverse actuation system for the Westinghouse AP1000 design certification amendment application*. USNRC. 8-11 March 2010. TRIM Ref. 2011/412986

68 *Notification of Regulatory Observation RO-AP1000-070 and Regulatory Observation Actions RO-AP1000-070.A1 to A3 – C&I use of SMART Devices in AP1000*. Letter from ND to AP1000 Project Front Office. WEC70155R. 11 March 2010. TRIM Ref. 2010/122641.

69 *Smart Sensors and Actuators Checklist WPD* FN-C 37194/36490R Issue 1.1. 3 August 2011. TRIM Ref. 2011/420223

70 *RO70 Partial Response - SMART Device Qualification Plan*. Letter from AP1000 Project Front Office to ND. UN REG WEC 000409. Westinghouse Electric Company LLC. 29 October 2010. TRIM Ref. 2010/548434.

71 *RO70 Full Response*. Letter from AP1000 Project Front Office to ND. UN REG WEC 000435. 30 November 2010. Westinghouse Electric Company LLC. TRIM Ref. 2010/606366.

72 *TQ-AP1000-1174. Westinghouse Response to TQ.* See Ref. 7.

73 *Review of the C&I Systems Important to Safety – UK AP1000*. Task 16: 37194-37195R . Issue 3.0. 3 August 2011. TRIM Ref. 2011/420333.

74 *Plan for Independent Assessment of AC160 to be used in UK AP1000 PMS*. Letter from AP1000 Project Front Office to ND. UN REG WEC 000411. 01 November 2010. TRIM Ref. 2010/549248.

75 *Independent Assessment of PMS Basis of Safety Case, Reviewers, and Schedule*. Letter from AP1000 Project Front Office to ND. UN REG WEC 000424. 09 November 2010. Westinghouse Electric Company LLC. TRIM Ref. 2010/562445.

76 *July C&I Action Item Closeout Letter.* Letter from AP1000 Project Front Office to ND. UN REG WEC 000284. Westinghouse Electric Company LLC. 30 July 2010. TRIM Ref. 2010/344215.

77 *WEC Commitment to Use MALPAS for AC160 Function Chart Analysis*. Letter from AP1000 Project Front Office to ND. UN REG WEC 000444. 9 December 2010. Westinghouse Electric Company LLC. TRIM Ref. 2010/623606.

78 *United Kingdom AP1000 Independent Assessment Report on the UKP-PMS-GLR-001 Protection and Safety Monitoring System Safety Case Basis*. UKP-GW-GL-001 Revision 0. Westinghouse Electric Company LLC. December 2010. TRIM Ref. 2011/76580.

79 *NII GDA Step 4 Technical Review - C&I. Calculated Trips – WPD Notes & Checklist.* S.P. 1440.074.011 Issue 1.2, 1 August 2011. Altran Praxis. TRIM Ref. 2011/406342.

80 *TQ-AP1000-788. Westinghouse Response. Calculated Trip Checklist.* See Ref. 7.

81 *Notification of Regulatory Observation RO-AP1000-071 and Regulatory Observation Actions RO-AP1000-070.A1 to A4 – C&I Adequacy of the DAS Architecture AP1000*. Letter from ND to AP1000 Project Front Office. WEC70156R. 11 March 2010. TRIM Ref. 2010/122710.

82 *RO 81: CIM-DAS Diversity Full Response*. Letter from AP1000 Project Front Office to ND. UN REG WEC 000366. 30 September 2010. TRIM Ref. 2010/485423.

83 *Review of the System-Level Architecture. Task 17: FN-C 37194-37165R*. Issue 3.0. 3 August 2011. TRIM Ref. 2011/420312

84 *AP1000 PRA Control and Instrumentation Sensitivity Cases Quantification*. APP-PRA-GSC-254 Revision 1. Westinghouse Electric Company LLC. 2009 TRIM Ref. 2011/76414.

85 *Step 4 Probabilistic Safety Analysis Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-003 Revision 0. TRIM Ref. 2010/581527.

86 *Step 4 Fault Studies Assessment of the Westinghouse AP1000® Reactor – Design Basis Faults*. ONR Assessment Report ONR-GDA-AR-11-004a Revision 0. TRIM Ref. 2010/581406.

87 *Notification of Regulatory Observaton RO-AP1000-081 and Regulatory Observation Action RO-AP1000-081.A1 C&I CIM – DAS Diversity AP1000*. WEC70184R. Letter from ND to Westinghouse Electric Company LLC. May 2010. TRIM Ref. 2010/234630.

88 *RO-AP1000-82. Spurious Operation of PMS.* Nuclear Directorate Letter UN WEC70189R. See Ref. 7.

89 *RO-AP1000-82. Westinghouse Response. Spurious Operation of PMS.* Westinghouse Letter UN WEC00392. See Ref. 7.

90 *TQ-AP1000-942. Westinghouse Response to TQ.* See Ref. 7.

91 *Guidance on means to achieve system diversity: DISPO 6 view. Bev Littlewood, Peter Popov, Lorenzo Strigini*. Version V1.1 PP_DISPO6_01. 17 March 2009. TRIM Ref. 2011/401667.

92 Review of the d*iversity of those systems contributing to the implementation of Category A functions – UK AP1000.* Task 18: FN-C 37194-65383R. Issue 4.0. 3 August 2011. TRIM Ref. 2011/

93 *Safety Assessment Principles Roadmap for AP1000 Design*. UKP-GW-GL-710 Section C Revision 2. Westinghouse Electric Company LLC. 28 July 2008. TRIM Ref. 2011/384432.

94 *UK Generic Design Assessment: Strategy for working with overseas regulators*. HSE. March 2009. www.hse.gov.uk/newreactors/ngn04.pdf.

95 *Westinghouse PMS Deviation Matrix FN-C 37194/36869R*. Issue 6.0. 4 August 2011. TRIM Ref. 2011/420293

96 *Review of Final PCSR in GDA for UK AP1000 – Step 4 Task 21 Report FN-C* 37194/37596R. Issue 1.0. 22 June 2011. TRIM Ref. 2011/420356

97 *Step 4 Cross-cutting Topics Assessment of the Westinghouse AP1000® Reactor*. ONR Assessment Report ONR-GDA-AR-11-016 Revision 0. TRIM Ref. 2010/581515.

98 *United Kingdom AP1000 Component Interface Module Safety Case Basis*. UKP-PMS-GLR-002 Revision 0. Westinghouse Electric Company LLC. November 2010. TRIM Ref. 2011/82119.

99 *Preferred Vendors List* UKP-GW-J0Y-002 Westinghouse Electric Company LLC. To be provided in response to GDA Issue GI-AP1000-CI-05.

100 *Justification of Class 1 SMART-Devices* UKP-GW-J0Y-004 Westinghouse Electric Company LLC. To be provided in response to GDA Issue GI-AP1000-CI-05.

101 *Justification of Class 2 & 3 SMART-Devices* UKP-GW-J0Y-005 Westinghouse Electric Company LLC. To be provided in response to GDA Issue GI-AP1000-CI-05.

102 *AP1000 SMART-Device Justification Plan* UKP-GW-GLR-017 Revision 0 Westinghouse Electric Company LLC. November 2010. TRIM Ref. 2011/82103.

103 *NII GDA Technical Review - C&I SAP Compliance Assessment for AP1000* - S.P1440.41.60, Issue 2.1, 7 January 2010. TRIM Ref. 2011/220543

Table 4

Relevant Safety Assessment Principles for C&I Considered During GDA Step 4

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 and standards
ECS.2	Safety classification of structures, systems and components
ECS.3	Standards
ECS.4	Codes and standards
ECS.5	Use of experience, tests or analysis
EQU - Equipment qualification	
EQU.1	Qualification procedures
EDR - Design for reliability	
EDR.1	Failure to safety
EDR.2	Redundancy, diversity and segregation
EDR.3	Common cause failure
EDR.4	Single failure criterion
ERL - Reliability claims	
ERL.1	Form of claims
ERL.2	Measures to achieve reliability
ERL.3	Engineered safety features
ERL.4	Margins of conservatism
ECM - Commissioning	
ECM.1	Commissioning testing
EMT - Maintenance Inspection and Testing	
EMT.1	Identification of requirements
EMT.2	Frequency
EMT.3	Type-testing
EMT.4	Validity of equipment qualification

Table 4

Relevant Safety Assessment Principles for C&I Considered During GDA Step 4

SAP No.	Assessment Topic / SAP Title
EMT.5	Procedures
EMT.6	Reliability claims
EMT.7	Functional testing
EAD - Aging and degradation	
EAD.1	Safe working life
EAD.2	Lifetime margins
EAD.3	Periodic measurement of material properties
EAD.5	Obsolescence
ELO - Layout	
ELO.1	Access
ELO.2	Unauthorised access
EHA - External and internal hazards	
EHA.10	Electromagnetic interference
ESS - Safety systems	
ESS.1	Requirement for safety systems
ESS.2	Determination of safety system requirements
ESS.3	Monitoring of plant safety
ESS.4	Adequacy of initiating variables
ESS.5	Plant interfaces
ESS.6	Adequacy of variables
ESS.7	Diversity in the detection of fault sequences
ESS.8	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.13	Confirmation of operating personnel
ESS.14	Prohibition of self-resetting of actions and alarms
ESS.15	Alteration of configuration, operational logic or associated data
ESS.16	No dependency on external sources of energy

Table 4

Relevant Safety Assessment Principles for C&I Considered During GDA Step 4

SAP No.	Assessment Topic / SAP Title
ESS.17	Failure identification
ESS.18	Failure independence
ESS.19	Dedication to a single task
ESS.20	Avoidance of connections to other systems
ESS.21	Reliability
ESS.22	Avoidance of spurious operation
ESS.23	Allowance for unavailability of equipment
ESS.24	Minimum operational equipment requirements
ESS.26	Maintenance and testing
ESS.27	Computer based safety systems
ESR - Control and instrumentation of safety related systems	
ESR.1	Provision in control rooms and other locations
ESR.2	Performance requirements
ESR.3	Provision of controls
ESR.4	Minimum operational equipment
ESR.5	Standards for computer based equipment
ESR.6	Power supplies
ESR.7	Communications systems
ESR.8	Monitoring of radioactive substances
ESR.9	Response of control systems to normal plant disturbances
ESR.10	Demands on safety systems in the event of control system faults
EES - Essential services	
EES.1	Provision
EES.2	Sources external to the site
EES.3	Capacity, duration, availability and reliability
EES.4	Sharing with other plants
EES.5	Cross-connections to other services
EES.6	Alternative sources
EES.7	Protection devices
EES.8	Sources external to the site

Table 4

Relevant Safety Assessment Principles for C&I Considered During GDA Step 4

SAP No.	Assessment Topic / SAP Title
EES.9	Loss of service
EHF - Human factors	
EHF.7	User interfaces
EHF.8	Personnel competence
ECV - Containment and ventilation	
ECV.6	Monitoring devices
ECV.7	Leakage monitoring
ERC - Reactor core	
ERC.2	Shutdown systems
DC - Decommissioning	
DC.1	Design and operation
DC.2	Decommissioning strategies

Annex 1

Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business - Control & Instrumentation – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-CI-001	Safety case argumentation and identification of evidence (CAE trail): • The Licensee shall produce a SAP conformance demonstration covering the full scope of SIS and platforms (i.e. by provision of Safety Case Maps for the 84 HSE C&I SAPs or other documentation as considered appropriate). • The Licensee shall ensure that the SAP conformance demonstration is, as appropriate, included in or referenced from the SIS and platform BSCs (see GDA Issues **GI-AP1000-CI-01, 06, 07, 08 and 09** in Sections 4.3 and 4.4). For further guidance see T13.TO1.01, T13.TO1.02 and T13.TO2.01 to T13.TO2.45 in Annex 3, T16.TO2.47 and T16.TO2.48 in Annex 6.	Prior to start of site nuclear island safety related concrete.
AF-AP1000-CI-002	The Licensee shall put in place an overarching Quality Assurance Programme (QAP) for the AP1000 C&I Systems Important to Safety development consistent with the WEC Quality Management System that either: • adopts appropriate IEC nuclear sector standards (Ref. 31): or • uses standards that are demonstrated to be equivalent to the IEC standards (e.g. through demonstrating the equivalence of WEC procedures and processes to the IEC standards). This QAP shall also identify the flow through of requirements to subcontractors (i.e. to instrument and equipment suppliers). For further guidance see T14.TO1.01, T14.TO2.01, T14.TO2.03 and T14.TO2.04 in Annex 4.	Long lead item procurement.

Annex 1

Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business - Control & Instrumentation – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-CI-003	The Licensee shall provide a safety case for the Radiation Monitoring System. The expectation is that the software development should comply with BS IEC 60880 unless it is demonstrated that this is not reasonably practicable and the use of the lower standard for developing software for Category B functions in accordance with BS IEC 62138 is fully justified.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.
AF-AP1000-CI-004	The Licensee shall ensure that C&I equipment installed as part of systems performing Category A or B functions is either: • assigned to a Class 1 or 2 system as appropriate and justified against relevant standards, or • a justification is provided for a assigning a lower or no-safety class. This not only applies to mechanical handling plant but also to any other equipment (for example the polar crane) where C&I equipment important to safety is embedded into or is part of the system.	Prior to install of polar crane.
AF-AP1000-CI-005	The Licensee shall produce a comprehensive demonstration of compliance with the five level 1 IEC nuclear sector C&I standards (i.e. BS IEC 61226, BS IEC 61513, BS IEC 60987, BS IEC 60880 and BS IEC 62138) for the AP1000 C&I Systems Important to Safety (SIS). The demonstration shall address: all relevant clauses; the operation and maintenance part of the SIS lifecycle; platforms and systems individually; and Class 3 systems. For further guidance see T14.TO1.01, T14.TO.03 and T14.TO2.04 in Annex 4, and T16.TO2.05 and T16.TO2.10 in Annex 6.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.

Annex 1

Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business - Control & Instrumentation – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-CI-006	The Licensee shall document the evidence supporting the claims (i.e. made in Ref. 33): • of equivalence of the IEEE standards and Regulatory guides with the level 2 IEC nuclear sector C&I standards; • that no gaps in compliance had been identified in WEC processes with the eleven level 2 standards claimed as similar to the IEC nuclear sector C&I standards; and • that the WEC processes meet the intent of the level 3 IEC nuclear sector C&I standards. For further guidance see T14.TO2.05 and T14.TO2.06 in Annex 4.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.
AF-AP1000-CI-007	The Licensee shall: • demonstrate that its Computer Based Systems Important to Safety (CBSIS) security management system aligns with appropriate standards such as ISO/IEC 27001 (Ref. 56); and • implement a CBSIS security assessment methodology that uses, or is equivalent to, the UK Government's standard methodology (Ref. 57).	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.
AF-AP1000-CI-008	The Licensee shall ensure a safety case is produced for the: In-core Instrumentation System; Turbine Control System; and Special Monitoring System.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.

Annex 1

Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business - Control & Instrumentation – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-CI-009	The Licensee shall produce a comprehensive demonstration that the Added Quality Demonstration compensatory measures (i.e. the use of operating history, testing and static analysis) have adequately addressed the gaps identified during the qualification exercise for the original development of the AC 160 version 1.3/0. For further guidance see T15.TO1.03, T15.TO2.01 a, b and c, T15.TO2.03, T15.TO2.07, T15.TO2.08, T15.TO2.32, and T15.TO2.39 b and c in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.
AF-AP1000-CI-010	The Licensee shall produce a safety justification for each Programmable Complex Electronic Component (PCECs) used in all Systems Important to Safety. The Licensee shall identify any deviations (i.e. gaps) from production excellence (as judged against an agreed standard) and demonstrate how the compensatory measures have adequately closed the gaps. This shall include demonstrating how test scripts were derived (e.g. from the requirements) and completion of the PCEC checklist. For further guidance see T15.TO2.01 b and d, T15.TO2.08, T15.TO2.27 and T15.TO2.39 a, b and c in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.

Annex 1

Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business - Control & Instrumentation – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-CI-011	The Licensee shall substantiate the claim of IEC 60880 compliance for the changes made to the AC160 to create: • the AC 160 V1.3/0 nuclear baseline from the V1.2 software; and • each subsequent AC 160 release (i.e. versions from V1.3/0 to V1.3/8). The Licensee shall document the change process used to create each of the software versions referenced above and demonstrate its adequacy. The Licensee shall ensure the demonstration of compliance with IEC 60880 addresses all relevant clauses such as change management, configuration control, software build, verification and test. The Licensee shall demonstrate that the tests adequately addressed the modifications (e.g. the tests addressed the changes to the requirements and provided adequate code coverage). For further guidance see T15.TO2.05, T15.TO2.06, T15.TO2.28, T15.TO2.34, T15.TO2.39 b, c and d, and T15.TO2.46 in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.
AF-AP1000-CI-012	The Licensee shall ensure that the adequacy of random access and other memory checking is substantiated in the BSC along with the operation of the distributed interpreter and the determinism of the communication links. For further guidance see T15.TO2.43 and T15.TO2.63 a and b in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.
AF-AP1000-CI-013	The Licensee shall determine and justify the reliability target of the Component Interface Module (CIM) in the AP1000 and demonstrate the adequacy of the CIM production processes in relation to the reliability target.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.

Annex 1

Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business - Control & Instrumentation – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-CI-014	The Licensee shall provide a comprehensive demonstration of the fitness for purpose of the Component Interface Module development process that addresses, amongst others: 1) requirements identification and traceability, 2) configuration management and change control, 3) verification and validation, and 4) staff independence. For further guidance in relation to 1) see T15.TO2.10b and c, T15.TO2.15a, and T15.TO2.42a and b; 2) see T15.TO2.16; 3) see T15.TO1.10c, d and g, T15.TO2.10c, T15.TO2.11, T15.TO2.12 and T15.TO2.42c; and 4) see T15.TO1.10b and T15.TO2.11 in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.
AF-AP1000-CI-015	The Licensee shall: 1) document in detail the areas for improvement established in WEC's self-assessment of the Component Interface Module development; 2) confirm the adequacy of the WEC assessment; and 3) demonstrate that the programme of compensatory measures has successfully addressed the areas for improvement.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.
AF-AP1000-CI-016	The Licensee shall demonstrate that an adequate independent verification and validation exercise has been applied to the Component Interface Module (e.g. by comparison with good practice represented by IEC standards). The demonstration should highlight the diverse nature of the exercise including use of diverse tools, simulations and test vectors.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.
AF-AP1000-CI-017	The Licensee shall ensure that the non-compliances raised by the US NRC (Ref. 67) in respect of the Component Interface Module development have been resolved to the Licensee's satisfaction.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.
AF-AP1000-CI-018	The Licensee shall ensure: the role of the complex software tools used to support the Component Interface Module development (e.g. for production of the Field Programmable Gate Array's Hardware Description and for testing) is identified; the tools have been justified as suitable for Class 1 development; and the tools are placed under configuration control. For further guidance see T15.TO1.10 e and f in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.

Annex 1

Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business - Control & Instrumentation – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-CI-019	Licensee shall substantiate the adequacy of coverage of the diagnostics and self-test features of the Component Interface Module. For further guidance see T15.TO1.06 b) and T15.TO2.62 in Annex 5.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.
AF-AP1000-CI-020	The Licensee shall ensure that: i) the DAS BSC justifies the adequacy of the development processes used for the 7300 series boards used in the DAS application, and ii) claims of proven-in-use / reliance on operating history are made explicit in the BSC. For further guidance see T15.TO2.14, T15.TO2.16, T15.TO2.21 and T15.TO2.53 in Annex 5.	Prior to nuclear island safety related concrete.
AF-AP1000-CI-021	The Licensee shall ensure that the analysis of the 7300 board failure modes and reliability is completed and documented as part of the DAS platform substantiation. For further guidance see T15.TO2.24, T15.TO2.25 and T15.TO2.26 in Annex 5.	Prior to nuclear island safety related concrete.
AF-AP1000-CI-022	The Licensee shall ensure that the Ovation platform claims identified in the response to RO 78 (Ref. 46) provide a complete safety argument. The Licensee shall identify the evidence supporting the claims by reference to documents that substantiate the claims. The Licensee shall ensure that the claims-arguments-evidence trail is presented in or referenced from the PCSR / safety case.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.
AF-AP1000-CI-023	The Licensee shall ensure there is an adequate safety case for in-core instrumentation sensors and other sensors used in Systems Important to Safety. This shall include a demonstration of conformance to relevant IEC standards. For further guidance see T13.TO2.46 in Annex 3.	Prior to C&I delivery to site.
AF-AP1000-CI-024	The Licensee shall demonstrate that the differences of functional coverage across the PMS Divisions do not give rise to any safety concerns (such as an inability to meet the reliability requirements or the single failure functional criterion requirements) when failures occur within a Division, or any Division is taken out of service for maintenance. For further guidance see T16.TO2.07 in Annex 6.	Prior to nuclear island safety related concrete.

Annex 1

Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business - Control & Instrumentation – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-CI-025	The Licensee shall complete the compensating measures identified in the "deviation" matrix (Ref. 95) for the PMS and its platform, and include the matrix as evidence of compliance with good practice (e.g. as defined in IEC nuclear sector C&I standards) in the BSC. For further guidance see also T16.TO2.02 in Annex 6.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.
AF-AP1000-CI-026	The Licensee shall demonstrate that the AF 100 bus and the associated communications equipment complies with Category A / Class 1 requirements, the communication response times are deterministic, and network traffic worst case loadings do not frustrate correct operation of the communications links. For further guidance, see T16.TO2.09 in Annex 6.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.
AF-AP1000-CI-027	The Licensee shall justify the acceptability of non Class 1 inputs to the PMS from the non Class 1 manual panels in the Remote Shutdown Room. For further guidance see T17.TO1.02b in Annex 7.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.
AF-AP1000-CI-028	The Licensee shall demonstrate the adequacy of the means of transferring control, and the safety functions, from the Main Control Room to the Remote Shutdown Room. This shall include demonstrating the arrangements meet the requirements of the SAPs EDR.4 (single failure proof) and ELO.2 (access to SIS); and similarly for transfer of control from the Main Control Room to any other remote or local control stations.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.

Annex 1

Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business - Control & Instrumentation – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-CI-029	The Licensee shall improve the content of the Safety Case Maps to: • make clear the CAE trail for the individual platforms and applications; • identify evidence by detailed references (i.e. by document section and paragraph); • ensure all elements of the SAPs are addressed; and • ensure the CAE trail presented in the SCMs is consistent with the safety arguments in the BSCs. For further guidance see T16.TO1.06 in Annex 6.	Prior to first nuclear island safety related concrete.
AF-AP1000-CI-030	The Licensee shall fully define the scope and programme for independent confidence building measures to be completed for the PMS and demonstrate that their coverage is appropriate in relation to the PMS integrity claims. For further guidance see T15.TO2.66 in Annex 5 and T16.TO1.02 in Annex 6.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.
AF-AP1000-CI-031	The Licensee shall demonstrate the appropriate and correct calculation of calculated parameters, and ESF actuation and reactor trip levels. The Licensee shall ensure that appropriate criteria and guidance are used in the demonstration (e.g. by completion of the calculated trip checklist and generation of a supporting justification). For further guidance see T16.TO2.08 in Annex 6.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.
AF-AP1000-CI-032	The Licensee shall demonstrate that the use of parameters calculated by the PMS, and used by both the PMS and PLS, cannot result in a common mode failure of the PMS and PLS (in particular where mitigation of the PLS failure would require correct operation of the PMS). For further guidance see T17.TO2.02b in Annex 7.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.

Annex 1

Assessment Findings to be Addressed During the Forward Programme as Normal Regulatory Business - Control & Instrumentation – AP1000

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-AP1000-CI-033	The Licensee shall produce a full set of AP1000 development records that demonstrate compliance with the development processes. This should include evidence of requirements traceability, configuration control, test planning, and review and verification records. For further guidance see T16.TO2.06 in Annex 6.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.
AF-AP1000-CI-034	The Licensee shall ensure that an overall demonstration of the adequacy of the overall C&I system architecture is produced. This demonstration should cover categorisation of C&I functions, assignment of functions to C&I SIS, independence and segregation requirements, need for diversity and robustness to data communication link failures such that a failure in a lower safety class system cannot frustrate the correct operation of a higher class system. The demonstration shall include consideration of all SIS elements including input and output devices, and the potential for CCF of multiple SIS as a result of use of common elements (e.g. sensors, possibly smart) across SIS. For further guidance see T17.TO1.02, T17.TO2.01, T17.TO2.02 and T17.TO2.03 in Annex 7.	Prior to nuclear island safety related concrete.
AF-AP1000-CI-035	The Licensee shall ensure that the safety case is updated to incorporate the PSA sensitivity study and its impact on C&I SIS reliability targets into the baseline model of the AP1000 PSA for the UK. For further guidance see T18.TO2.12 in Annex 8.	Prior to nuclear island safety related concrete.
AF-AP1000-CI-036	The Licensee shall provide a detailed diversity analysis of the PMS / PLS applications and AC 160 / Ovation platforms. For further guidance see T18.TO2.11, T18.TO2.20 and T18.TO2.24 in Annex 8.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.
AF-AP1000-CI-037	The Licensee shall, when selecting platforms for systems that are currently out of scope, review the potential for common cause failure of SIS (e.g. as a result of the use of common SIS platforms or platforms with common features). For further guidance see T18.TO2.18 in Annex 8.	Prior to mechanical, electrical and C&I safety systems, structures and somponents delivery to site.

Annex 1

Note: It is the responsibility of the Licensees / Operators to have adequate arrangements to address the Assessment Findings. Future Licensees / Operators can adopt alternative means to those indicated in the findings which give an equivalent level of safety.

For Assessment Findings relevant to the operational phase of the reactor, the Licensees / Operators must adequately address the findings during the operational phase. For other Assessment Findings, it is the regulators' expectation that the findings are adequately addressed no later than the milestones indicated above.

Annex 2

GDA Issues – Control and Instrumentation – AP1000

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

DAS – ADEQUACY OF SAFETY CASE

GI-AP1000-CI-01 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-01**	**GDA Issue Action Reference**	**GI-AP1000-CI-01.A1**
GDA Issue	Westinghouse has proposed design changes to the DAS secondary protection system, as a result the DAS design is not complete and this has lead to the absence of safety case argumentation and evidence to substantiate the DAS design. Westinghouse has provided an initial basis of safety case (BSC) for the DAS and ONR's assessment has shown that this broadly aligns with our expectations. However, Westinghouse needs to respond to ONR's observations on the BSC, progress the detailed design, complete the safety case, provide the evidence identified in the safety case and introduce the design change proposal. For further guidance, see T15.TO2.14, T15.TO2.16, T15.TO2.18 to 26 and T15.TO2.54 in Annex 5, and also T16.TO1.03 and its associated TO2s, T16.TO1.04, T16.TO2.17, and T16.TO2.43 in Annex 6.		
GDA Issue Action	Westinghouse to formally introduce the change to the architecture and technology of the DAS via the design change process (DCP). The revised DAS has to be formally introduced and the safety documentation amended accordingly. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

DAS – ADEQUACY OF SAFETY CASE

GI-AP1000-CI-01 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-01**	**GDA Issue Action Reference**	**GI-AP1000-CI-01.A2**
GDA Issue Action	Westinghouse to provide the basis of safety case for the completed design of the DAS. The form and content of the BSC for the completed design is indicated below, the interim BSCs should also record in principle the methodology by which the missing design information and substantiation will be included to demonstrate the adequacy of the DAS and to justify that sufficient information will be available in a timely fashion for assessment by ONR. The BSC should start by identifying the safety principles and standards (i.e. company, national and international) that WEC has adopted for the equipment / system. The BSC should identify the arguments for assigning safety functions and performance requirements to the equipment / system in compliance with the categorisation and classification principles and standards. The BSC demonstration of compliance with SAPs and standards needs to show that the development practices are consistent with modern standards and the declared practices (e.g. in procedures) have been adhered to. Compensatory measures are required to address gaps in the compliance demonstration. The BSC should describe the AP1000 C&I project QA arrangements and certification (e.g. to ISO 9001). The BSC should include a clear description of the interface to the equipment / system supplier (and any other suppliers) and outline their QA arrangements and their adequacy. The BSC should describe the equipment / system, and identify the major elements (such as sensors, input/output and logic cards, and actuators) and include the demonstration of their adequacy. The BSC or other documents referenced from the BSC should address the system integration process including the intended factory and commissioning tests, and environmental qualification. The BSC should describe future work related to site construction and commissioning activities, and identify when the evidence related to these activities will be produced. For completeness, the BSC should also specify through life operating and maintenance requirements including the minimum equipment availability requirements, and the scope and frequency of any proof testing. The BSC should identify any supporting analysis such as hazards analysis, FMEAs, reliability analysis, environmental qualification, and link them to the claims made in the safety demonstration. The BSC should identify the use of defensive design and fault revealing techniques. The BSC should identify the pedigree of any COTS and pre-developed components and provide a demonstration of the adequacy of the development arrangements. For older		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

DAS – ADEQUACY OF SAFETY CASE

GI-AP1000-CI-01 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-01**	**GDA Issue Action Reference**	**GI-AP1000-CI-01.A2**
	components the safety argument might involve use of proven in use arguments and testing rather than a production excellence argument. In either case any compensatory measures undertaken to address shortfalls should be identified in the safety demonstration. The BSC should demonstrate how the design and implementation of the equipment using complex / programmable, components, e.g. microprocessors, ASICs, and Field Programmable Gate Arrays complies with relevant WEC safety principles and standards. Given the programmable nature of such complex devices, the justification should draw on SAP ESS.27 a special case procedure for the demonstration of safety that involves the presentation of an argument of production excellence and implementation of independent confidence building measures. Where complex hardware is involved, the BSC should identify how the safety demonstration conforms to ESS.21 and the need for measures such as independent third party assessment. The BSC should include a plan that shows the forward activities, and production of related safety case documentation and evidence. Interim BSCs should be provided, particularly for large complex systems. A BSC for the completed design[1] should be submitted as soon as reasonably practicable before permission to commence nuclear site construction is sought. A BSC for installation and commissioning would be expected before equipment is delivered to site. Notes 1. Completed design – The design is complete at the point where the: • requirements, specifications, and implementation details (e.g. software coding and circuit diagrams etc.) have been completed; • production verification and validation activities (i.e. prior to delivery to site) have been completed; • prototype equipment has been produced and subject to performance and qualification testing; With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

DAS – ADEQUACY OF ARCHITECTURE

GI-AP1000-CI-02 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-02**	**GDA Issue Action Reference**	**GI-AP1000-CI-02.A1**
GDA Issue	ONR sought clarity regarding the adequacy of the DAS (the secondary protection system) 2 out of 2 operating philosophy. In response Westinghouse has proposed significant changes to the architecture of the DAS (i.e. from a 2 channel 2oo2 voted system to a system whose logic is a combination of 2oo3 or 1oo2 twice voting). The expectation is that this modified architecture will allow the DAS to remain in service during power operation but this needs to be substantiated as the detailed design and reliability analyses are completed. The substantiation should also demonstrate that both the automatic and manual DAS can achieve their declared reliability targets. For further guidance, see T16.TO1.04 and T16.TO2.17 in Annex 6.		
GDA Issue Action	Provide a substantiation that the automatic DAS remains in service during reactor power operation including meeting the requirements for maintenance and proof testing. The DAS forms part of the reactor protection system and Westinghouse had identified that the DAS would be a two channel system requiring a 2oo2 vote and positive actuation to trip. The DAS automatic trip function would not be available during reactor operation when test and maintenance activities are undertaken as the channel is in bypass and the 2oo2 logic retained. The DAS Engineered Safeguard Features (ESF) manual controls would also be powered down during reactor power operation. ONR identified that this architecture and mode of system operation appeared contrary to a number of the SAPs associated with protection systems, e.g. ESS 21 & EDR 1, and ESS 23 for maintenance, and for systems providing the ESF, e.g. ESS 8 & 9 and ERL 3. Westinghouse has proposed, a change to the DAS architecture changing the required automatic logic from 2oo2 logic to a combination of 2003 and 1oo2 twice logic. ONR has reviewed the change proposal noting that it in principle addresses the concerns raised and has provided comments to Westinghouse to this effect. Note: The revised DAS has to be formally introduced, its design completed, see GI-AP1000-CI-01.A1 & A2, to allow the necessary analysis to be completed to substantiate that the DAS is available at all times during power operation. The substantiation should be included in the basis of safety case for the DAS. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
DAS – ADEQUACY OF ARCHITECTURE
GI-AP1000-CI-02 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-02**	**GDA Issue Action Reference**	**GI-AP1000-CI-02.A2**
GDA Issue Action	Provide a substantiation that the automatic and the manual DAS meets their reliability targets. The revised DAS has to be formally introduced, its design completed, see GI-AP1000-CI-01.A1 & A2, to allow the necessary analysis to be completed to substantiate that both the automatic and manual parts of the DAS meet their reliability targets. Note: the substantiation should be included in the basis of safety case for the DAS. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
DAS – ADEQUACY OF ARCHITECTURE
GI-AP1000-CI-02 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	Electrical		
GDA Issue Reference	**GI-AP1000-CI-02**	**GDA Issue Action Reference**	**GI-AP1000-CI-02.A3**
GDA Issue Action	Identify and provide a description of the sources of electric power for the DAS and their physical location on the plant. This should include the safety class of the supply, the source of supply including the division providing the supply, supply voltage and capacity, and loads supplied. For battery backed supplies the battery operating time is also required. For the DAS dedicated battery supplies the location of the equipment (batteries and chargers) is required along with their safety class, loads supplied and battery operating time. The primary source of power should be described as part of the response above. Other sources of power required by the DAS to operate should be described, for example for firing the squib valves or hydrogen igniters. The details required are as indicated above. The descriptions should be supported by a substantiation of the adequacy of the supplies including their qualification, capacity and a demonstration that supply performance is consistent with the reliability claims on and the availability / endurance of the DAS. Note: the description and substantiation of the adequacy of the supplies should be included in the basis of safety case for the DAS. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

DIVERSITY OF PLS, PMS (INC CIM) AND DAS

GI-AP1000-CI-03 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-03**	**GDA Issue Action Reference**	**GI-AP1000-CI-03.A1**
GDA Issue	ONR identified an apparent lack of diversity of the primary protection system PMS (the CIM) and the diverse secondary protection system DAS. Diversity between the PMS (CIM) and DAS was a significant issue as it was proposed to use the same FPGA component suppliers and application developers. The change of choice of DAS platform to a conventional discrete electronic one provided a significant step forwards. Nevertheless a detailed diversity analysis is required for the DAS against the PLS/DDS and the PMS. ONR's expectation is that these diversity analyses will be set out in an appropriate basis of safety case. For further guidance, see T18.TO1.01, T18.TO2.06, T18.TO2.11, T18.TO2.19, T18.TO2.21 and T18.TO2.25 in Annex 8.		
GDA Issue Action	Provide a detailed diversity analysis for the DAS (7300 series) against the PLS/DDS (Ovation) and the PMS (Common Q). Defence against failure of the control system PLS (and others such as the TOS) is provided by the PMS primary and DAS secondary protection systems; further, defence against PMS failure is provided by DAS. In order for such defences to be effective the systems need to have properties including independence and diversity. The diversity of the PMS's CIM component and the DAS was raised a number of times and challenged as the CIM and DAS were to be implemented: by the same application developer; in the same FPGA technology, and using FPGAs and development tools from the same supplier. In response Westinghouse advised that the technology choice for the DAS would be changed to use its 7300 series equipment based primarily on analogue technology. This was seen as a significant step forward; however, once the DAS and PLS designs are complete a detailed diversity analysis will be required for the PMS and DAS and for the PLS and DAS. Note the analysis should be included in a basis of safety case document, for example, that for the DAS. The revised DAS technology choice to be formally introduced, its design completed to allow the necessary detailed diversity analysis to be completed to substantiate that it is diverse from both the PLS/DDS and PMS. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
PMS SPURIOUS OPERATION
GI-AP1000-CI-04 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	Fault Studies		
GDA Issue Reference	**GI-AP1000-CI-04**	**GDA Issue Action Reference**	**GI-AP1000-CI-04.A1**
GDA Issue	The PMS has the capability to actuate any of the Engineered Safety Features (ESF) on the AP1000. This includes the potential to spuriously actuate the Automatic Depressurisation System (ADS) valves or the containment recirculation valves. The spurious operation of these functions has the potential to initiate safety significant transients such as a large LOCA or drainage of the in-containment refuelling water storage tank (IRWST). Westinghouse needs to provide a design basis safety case covering such spurious actuations. Westinghouse has proposed implementing an interlock/blocker to reduce the ADS spurious initiating frequency. Westinghouse needs to formally introduce the design change, complete the design and provide a substantiation of the claims made on the blocker device. For further guidance, see T17.TO1.01 in Annex 7.		
GDA Issue Action	Westinghouse to provide a design basis safety case covering spurious PMS actuation of the ADS valves. The safety case will need to demonstrate that the ADS interlock/blocker device provides adequate protection against such faults or provide additional protection or justification as to why the position is acceptable. For the US design the PMS reliability claim is such that these events are outside the plant design basis; however, the UK design makes a lower claim on the PMS reliability, hence, there is a higher assumed dangerous failure rate bringing these events within the design base. The safety case will need to recognise the effectiveness of the blocker device may well be limited by the reliability of the CIM and so additional protection might be required. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
PMS SPURIOUS OPERATION
GI-AP1000-CI-04 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-04**	**GDA Issue Action Reference**	**GI-AP1000-CI-04.A2**
GDA Issue Action	Westinghouse is required to provide a design basis safety case covering spurious operation of the containment recirculation squib valves. Westinghouse needs to demonstrate that adequate protection is provided or propose possible design changes to reduce the initiating frequency of the event and/or provide additional protection. The safety case needs to provide a full deterministic and probabilistic assessment to demonstrate that the risk of serious consequences following spurious operation of the recirculation valves is below the design basis sequence cut-off frequency of 10^{-7} per year while ensuring the reliability of recirculation valves to perform their important safety function has not been significantly affected. Westinghouse has identified that spurious operation of the PMS can potentially result in the inadvertent opening of the containment recirculation squib valves causing the draining of the IRWST. If these valves are not isolated by the operator such a fault has the potential to: • flood the containment sump (possibly resulting in RCP trip and consequential reactor trip), and; • result in the consequential failure of the PRHR heat exchanger and the IRWST safety injection system which are the two Class A1 post-trip cooling systems on the AP1000. It is not clear that this situation meets Westinghouse's own design criteria, which is that for every design basis fault there should be at least one Class A1 safety system to protect against the fault and that operator actions should not be required for at least 72 hours. Should Westinghouse choose to implement the blocker device in a similar manner to that applied on the ADS valves then the safety case needs to recognise that the effectiveness of the blocker device may be limited by the reliability of the CIM and so additional protection may well be required. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
PMS SPURIOUS OPERATION
GI-AP1000-CI-04 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-04**	**GDA Issue Action Reference**	**GI-AP1000-CI-04.A3**
GDA Issue Action	Westinghouse to formally introduce the change to the PMS design to introduce the interlock/blocker on the ADS valves via the design change process (DCP). With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
PMS SPURIOUS OPERATION
GI-AP1000-CI-04 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-04**	**GDA Issue Action Reference**	**GI-AP1000-CI-04.A4**
GDA Issue Action	Westinghouse to complete the design of the interlock/blocker and substantiate it for its intended role. Westinghouse presented, in three notes, a concept design for interlocking/blocking the actuation of the ADS 1 to 4 valves using a signal based on measurement of the level of the core makeup tank fed into the existing PMS CIM Z port. ONR reviewed the design concept and comments were provided to Westinghouse. However, the design and design substantiation need to be completed. The design substantiation should include an evaluation of the ADS 1 to 4 valve spurious operation rates (accounting for sensor failure and PMS test and maintenance activities). With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

SMART DEVICE JUSTIFICATION FOR USE

GI-AP1000-CI-05 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	Electrical		
GDA Issue Reference	**GI-AP1000-CI-05**	**GDA Issue Action Reference**	**GI-AP1000-CI-05.A1**
GDA Issue	ONR raised the issue that Westinghouse's approach to SMART devices (i.e. ones containing programmable elements) was not developed; WEC made the proposal for the development of an integrated approach across all technical areas. The response is in principle acceptable but requires implementation and a supporting demonstration of its adequacy. ONR will need to see evidence of the approach actually being implemented through, for example, its application to sample devices at different classes. For further guidance, see T15.TO2.29 in Annex 5.		
GDA Issue Action	Westinghouse to provide copies of the procedures (UKP-GW-J0Y- 002, 004 & 005) supporting the justification process (UKP-GW-GLR-017 rev 0) for review. Westinghouse has identified that it is unlikely smart devices will be used in safety equipment within the containment such as the class 1 PMS, they are not expected to tolerate the harsh environmental conditions) but that SMARTs would be used by preference in class 2 and 3 C&I systems and also in other systems including class 1 electrical power systems. ONR drew Westinghouse's attention to chapter 1.15 of the 2010 version of the document 'Licensing of safety critical software for nuclear reactors - Common position of seven European nuclear regulators and authorised technical support organisations' on smarts. Sections 1 and 2 give information on the background, section 3 identifies the common position taken by the organisations, while section 4 identifies recommended practices adopted by the UK Regulator among others. Westinghouse is required to describe its approach to justification of smarts and to demonstrate that it aligns with the identified common positions and recommended practices with justification of any variances. Westinghouse is also aware of the approach developed in the UK as part of the CINIF research programme including the use of the EMPHASIS tool. Westinghouse's proposal is, in principle, acceptable and the detailed review findings on the information presented will be recorded in the GDA Step 4 report. However, to complete the assessment the detailed evidence will need to be reviewed including: the three procedures (UKP-GW-J0Y- 002, 004 & 005) identified in the head document (UKP-GW-GLR-017 rev 0) supplied via letter 000435, and the evidence arising from application of the process to sample devices from the three different classes. The latter are to be agreed with ONR in advance. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
SMART DEVICE JUSTIFICATION FOR USE
GI-AP1000-CI-05 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	Electrical		
GDA Issue Reference	**GI-AP1000-CI-05**	**GDA Issue Action Reference**	**GI-AP1000-CI-05.A2**
GDA Issue Action	Westinghouse to provide the evidence from implementation of their smart device justification process as applied to sample devices agreed with ONR from the three Safety Classes. This is to include the output from implementation of the Westinghouse qualification procedures and completed "NII GDA Technical review – C&I Smart Sensor and Actuators Checklist" (Ref.69). With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

OVATION PLATFORM ADEQUACY OF SAFETY CASE

GI-AP1000-CI-06 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-06**	**GDA Issue Action Reference**	**GI-AP1000-CI-06.A1**
GDA Issue	ONR is seeking an adequate safety case for the Ovation platform that supports the Class 2 closed loop controls and the Class 3 manual controls and displays of AP1000. Westinghouse submitted information on the platform but progress on its assessment was delayed due to priority being given to topics relating to the protection systems including the PMS/CIM safety case, CIM/DAS diversity and PMS blocker. A basis of safety case for the Ovation platform and access to it supporting evidence is required. For further guidance, see T15.TO1.01 in Annex 5.		
GDA Issue Action	Westinghouse to facilitate ONR access in the UK to the detailed evidence used to support the basis of safety case for the Ovation platform. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

OVATION PLATFORM ADEQUACY OF SAFETY CASE

GI-AP1000-CI-06 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-06**	**GDA Issue Action Reference**	**GI-AP1000-CI-06.A2**
GDA Issue Action	Westinghouse to provide a basis of safety case (BSC) that includes a justification of the suitability of the Ovation platform for Class 2 and 3 systems. The BSC should start by identifying the safety principles and standards (i.e. company, national and international) that WEC has adopted for the equipment / system. The BSC should identify the arguments for assigning safety functions and performance requirements to the equipment / system in compliance with the categorisation and classification principles and standards. The BSC demonstration of compliance with SAPs and standards needs to show that the development practices are consistent with modern standards and the declared practices (e.g. in procedures) have been adhered to. Compensatory measures are required to address gaps in the compliance demonstration. The BSC should describe the AP1000 C&I project QA arrangements and certification (e.g. to ISO 9001). The BSC should include a clear description of the interface to the equipment / system supplier (and any other suppliers) and outline their QA arrangements and their adequacy. The BSC should describe the equipment / system, and identify the major elements (such as sensors, input/output and logic cards, and actuators) and include the demonstration of their adequacy. The BSC or other documents referenced from the BSC should address the system integration process including the intended factory and commissioning tests, and environmental qualification. The BSC should describe future work related to site construction and commissioning activities, and identify when the evidence related to these activities will be produced. For completeness, the BSC should also specify through life operating and maintenance requirements including the minimum equipment availability requirements, and the scope and frequency of any proof testing. The BSC should identify any supporting analysis such as hazards analysis, FMEAs, reliability analysis, environmental qualification, and link them to the claims made in the safety demonstration. The BSC should identify the use of defensive design and fault revealing techniques. The BSC should identify the pedigree of any COTS and pre-developed components and provide a demonstration of the adequacy of the development arrangements. For older components the safety argument might involve use of proven in use arguments and testing rather than a production excellence argument. In either case any compensatory measures undertaken to address shortfalls should be identified in the safety demonstration.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

OVATION PLATFORM ADEQUACY OF SAFETY CASE

GI-AP1000-CI-06 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-06**	**GDA Issue Action Reference**	**GI-AP1000-CI-06.A2**
	The BSC should demonstrate how the design and implementation of the equipment using complex / programmable, components, e.g. microprocessors, ASICs, and Field Programmable Gate Arrays complies with relevant WEC safety principles and standards. Given the programmable nature of such complex devices, the justification should draw on SAP ESS.27, a special case procedure for the demonstration of safety that involves the presentation of an argument of production excellence and implementation of independent confidence building measures. Where complex hardware is involved, the BSC should identify how the safety demonstration conforms to ESS.21 and the need for measures such as independent third party assessment. The BSC should include a plan that shows the forward activities, and production of related safety case documentation and evidence. Interim BSCs should be provided, particularly for large complex systems. A BSC for the completed design[1] should be submitted as soon as reasonably practicable before permission to commence nuclear site construction is sought. A BSC for installation and commissioning would be expected before equipment is delivered to site. Notes 1. Completed design – The design is complete at the point where the: • requirements, specifications, and implementation details (e.g. software coding and circuit diagrams etc.) have been completed; • production verification and validation activities (i.e. prior to delivery to site) have been completed; • prototype equipment has been produced and subject to performance and qualification testing; With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
DCIS ADEQUACY OF SAFETY CASE
GI-AP1000-CI-07 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-07**	**GDA Issue Action Reference**	**GI-AP1000-CI-07.A1**
GDA Issue	The AP1000 automatic controls and its manual controls and displays are in the DCIS (PLS/DDS). The systems have to be justified as Class 2 (PLS) and Class 3 (DDS) respectively as part of the plant safety case; this requires a new justification as the systems are given a non safety classification in the US. The justification is expected to be in the form of a basis of safety case supported by documented evidence substantiating the claims for the systems and their development. For further guidance, see T15.TO2.36 in Annex 5 and T16.TO1.05 and its associated TO2s, and T16.TO2.19 to 27 in Annex 6.		
GDA Issue Action	Westinghouse to facilitate ONR access in the UK to the detailed evidence used to support the basis of safety case for the PLS and DDS applications. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

DCIS ADEQUACY OF SAFETY CASE

GI-AP1000-CI-07 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-07**	**GDA Issue Action Reference**	**GI-AP1000-CI-07.A2**
GDA Issue Action	Westinghouse to provide a basis of safety case that includes a justification of the suitability of the PLS application at Class 2 (control) and the DDS application at Class 3 (manual control and display). The content of a BSC is outlined below. The BSC should start by identifying the safety principles and standards (i.e. company, national and international) that WEC has adopted for the equipment / system. The BSC should identify the arguments for assigning safety functions and performance requirements to the equipment / system in compliance with the categorisation and classification principles and standards. The BSC demonstration of compliance with SAPs and standards needs to show that the development practices are consistent with modern standards and the declared practices (e.g. in procedures) have been adhered to. Compensatory measures are required to address gaps in the compliance demonstration. The BSC should describe the AP1000 C&I project QA arrangements and certification (e.g. to ISO 9001). The BSC should include a clear description of the interface to the equipment / system supplier (and any other suppliers) and outline their QA arrangements and their adequacy. The BSC should describe the equipment / system, and identify the major elements (such as sensors, input/output and logic cards, and actuators) and include the demonstration of their adequacy. The BSC or other documents referenced from the BSC should address the system integration process including the intended factory and commissioning tests, and environmental qualification. The BSC should describe future work related to site construction and commissioning activities, and identify when the evidence related to these activities will be produced. For completeness, the BSC should also specify through life operating and maintenance requirements including the minimum equipment availability requirements, and the scope and frequency of any proof testing. The BSC should identify any supporting analysis such as hazards analysis, FMEAs, reliability analysis, environmental qualification, and link them to the claims made in the safety demonstration. The BSC should identify the use of defensive design and fault revealing techniques. The BSC should identify the pedigree of any COTS and pre-developed components and provide a demonstration of the adequacy of the development arrangements. For older components the safety argument might involve use of proven in use arguments and testing rather than a production excellence argument. In either case any compensatory measures undertaken to address shortfalls should be identified in the safety		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

DCIS ADEQUACY OF SAFETY CASE

GI-AP1000-CI-07 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-07**	**GDA Issue Action Reference**	**GI-AP1000-CI-07.A2**
	demonstration. The BSC should demonstrate how the design and implementation of the equipment using complex / programmable, components, e.g. microprocessors, ASICs, and Field Programmable Gate Arrays complies with relevant WEC safety principles and standards. Given the programmable nature of such complex devices, the justification should draw on SAP ESS.27 a special case procedure for the demonstration of safety that involves the presentation of an argument of production excellence and implementation of independent confidence building measures. Where complex hardware is involved, the BSC should identify how the safety demonstration conforms to ESS.21 and the need for measures such as independent third party assessment. The BSC should include a plan that shows the forward activities, and production of related safety case documentation and evidence. Interim BSCs should be provided, particularly for large complex systems. A BSC for the completed design[1] should be submitted as soon as reasonably practicable before permission to commence nuclear site construction is sought. A BSC for installation and commissioning would be expected before equipment is delivered to site. Notes 1. Completed design – The design is complete at the point where the: • requirements, specifications, and implementation details (e.g. software coding and circuit diagrams etc.) have been completed; • production verification and validation activities (i.e. prior to delivery to site) have been completed; • prototype equipment has been produced and subject to performance and qualification testing; With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

PMS ADEQUACY OF SAFETY CASE

GI-AP1000-CI-08 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-08**	**GDA Issue Action Reference**	**GI-AP1000-CI-08.A1**
GDA Issue	Shortfalls have been identified in the provision of a claims - argument - evidence structure for the PMS safety demonstration. The PMS is based on non safety equipment and requires an 'added quality' demonstration to be made; this demonstration has proved difficult to understand without a logically structured safety case. In response to our concerns WEC has produced a Basis of Safety Case (BSC) for the PMS covering both the platform and application development. Review of the BSC has identified a number of areas for improvement including, to the SAPs and IEC standards conformance demonstration, and justification of the scope and adequacy of the independent confidence building measures. The PMS safety case needs to incorporate the responses to the PMS related Assessment Findings identified in the main body of this Assessment Report and to reflect PMS development progress as the design is completed For further guidance, see T15.TO1.02, T15.TO1.03 T15.TO1.11 and their associated TO2s plus T15.TO2.36 and T15.TO2.43 in Annex 5, and also T16.TO1.01 and its associated TO2s, and T16.TO1.02, T16.TO2.07, T16.TO2.08, T16.TO2.09, T16.TO2.38, T16.TO2.42 and T16.TO2.45 in Annex 6.		
GDA Issue Action	Westinghouse to facilitate ONR access in the UK to the detailed evidence used to support the basis of safety case for the PMS. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT
GDA ISSUE
PMS ADEQUACY OF SAFETY CASE
GI-AP1000-CI-08 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-08**	**GDA Issue Action Reference**	**GI-AP1000-CI-08.A2**
GDA Issue Action	Westinghouse to provide a basis of safety case for the PMS that takes into account the expectations expressed below: The BSC should start by identifying the safety principles and standards (i.e. company, national and international) that WEC has adopted for the equipment / system. The BSC should identify the arguments for assigning safety functions and performance requirements to the equipment / system in compliance with the categorisation and classification principles and standards. The BSC demonstration of compliance with SAPs and standards needs to show that the development practices are consistent with modern standards and the declared practices (e.g. in procedures) have been adhered to. Compensatory measures are required to address gaps in the compliance demonstration. The BSC should describe the AP1000 C&I project QA arrangements and certification (e.g. to ISO 9001). The BSC should include a clear description of the interface to the equipment / system supplier (and any other suppliers) and outline their QA arrangements and their adequacy. The BSC should describe the equipment / system, and identify the major elements (such as sensors, input/output and logic cards, and actuators) and include the demonstration of their adequacy. The BSC or other documents referenced from the BSC should address the system integration process including the intended factory and commissioning tests, and environmental qualification. The BSC should describe future work related to site construction and commissioning activities, and identify when the evidence related to these activities will be produced. For completeness, the BSC should also specify through life operating and maintenance requirements including the minimum equipment availability requirements, and the scope and frequency of any proof testing. The BSC should identify any supporting analysis such as hazards analysis, FMEAs, reliability analysis, environmental qualification, and link them to the claims made in the safety demonstration. The BSC should identify the use of defensive design and fault revealing techniques. The BSC should identify the pedigree of any COTS and pre-developed components and provide a demonstration of the adequacy of the development arrangements. For older components the safety argument might involve use of proven in use arguments and testing rather than a production excellence argument. In either case any compensatory measures undertaken to address shortfalls should be identified in the safety demonstration.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

PMS ADEQUACY OF SAFETY CASE

GI-AP1000-CI-08 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-08**	**GDA Issue Action Reference**	**GI-AP1000-CI-08.A2**
	The BSC should demonstrate how the design and implementation of the equipment using complex / programmable, components, e.g. microprocessors, ASICs, and Field Programmable Gate Arrays complies with relevant WEC safety principles and standards. Given the programmable nature of such complex devices, the justification should draw on SAP ESS.27 a special case procedure for the demonstration of safety that involves the presentation of an argument of production excellence and implementation of independent confidence building measures. Where complex hardware is involved, the BSC should identify how the safety demonstration conforms to ESS.21 and the need for measures such as independent third party assessment. The BSC should include a plan that shows the forward activities, and production of related safety case documentation and evidence. Interim BSCs should be provided, particularly for large complex systems. A BSC for the completed design[1] should be submitted as soon as reasonably practicable before permission to commence nuclear site construction is sought. A BSC for installation and commissioning would be expected before equipment is delivered to site. Notes 1. Completed design – The design is complete at the point where the: • requirements, specifications, and implementation details (e.g. software coding and circuit diagrams etc.) have been completed; • production verification and validation activities (i.e. prior to delivery to site) have been completed; • prototype equipment has been produced and subject to performance and qualification testing; With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

CIM – ADEQUACY OF SAFETY CASE

GI-AP1000-CI-09 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-09**	**GDA Issue Action Reference**	**GI-AP1000-CI-09.A1**
GDA Issue	Shortfalls have been identified in the provision of a claims - argument - evidence structure in the CIM safety case. The CIM is a critical component of the primary protection system. It is based on Field Programmable gate array (FPGA) technology and is supplied by a company with little experience in the nuclear sector. In response to our concerns WEC has produced a Basis of Safety Case (BSC) for the CIM. Assessment of the BSC has identified a number of areas for improvement. The key areas for improvement are: • demonstration that the development process is compliant or equivalent to IEC standards; and • identification of the evidence to support the demonstration. The BSC should document the standards compliance and address issues related to use of tools and test coverage. The rigour of the safety demonstration provided in the BSC should reflect the reliability claim on the CIM. The CIM safety case needs to incorporate the responses to the CIM related Assessment Findings identified in the main body of this Assessment Report and to reflect CIM development progress as the design is completed. For further guidance, see T15.TO1.05, T15.TO1.06, T15.TO1.07, T15.TO1.08, T15.TO1.10 and their associated TO2s in Annex 5.		
GDA Issue Action	Westinghouse to facilitate ONR access in the UK to the detailed evidence used to support the basis of safety case for the CIM. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

CIM – ADEQUACY OF SAFETY CASE

GI-AP1000-CI-09 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-09**	**GDA Issue Action Reference**	**GI-AP1000-CI-09.A2**
GDA Issue Action	Westinghouse to provide the basis of safety case for the completed design of the CIM. The expectation is that the observations already provided will be taken into account along with those identified in the main body of this Assessment Report and in particular account will be taken of the CIM's reliability requirement, and remedial action including IV&V undertaken by Westinghouse. The detailed evidence above will be assessed as part of the CIM BSC review. The expectations of the form and a basis of safety case for the CIM are set down below: The BSC should start by identifying the safety principles and standards (i.e. company, national and international) that WEC has adopted for the equipment / system. The BSC should identify the arguments for assigning safety functions and performance requirements to the equipment / system in compliance with the categorisation and classification principles and standards. The BSC demonstration of compliance with SAPs and standards needs to show that the development practices are consistent with modern standards and the declared practices (e.g. in procedures) have been adhered to. Compensatory measures are required to address gaps in the compliance demonstration. The BSC should describe the AP1000 C&I project QA arrangements and certification (e.g. to ISO 9001). The BSC should include a clear description of the interface to the equipment / system supplier (and any other suppliers) and outline their QA arrangements and their adequacy. The BSC should describe the equipment / system, and identify the major elements (such as sensors, input/output and logic cards, and actuators) and include the demonstration of their adequacy. The BSC or other documents referenced from the BSC should address the system integration process including the intended factory and commissioning tests, and environmental qualification. The BSC should describe future work related to site construction and commissioning activities, and identify when the evidence related to these activities will be produced. For completeness, the BSC should also specify through life operating and maintenance requirements including the minimum equipment availability requirements, and the scope and frequency of any proof testing. The BSC should identify any supporting analysis such as hazards analysis, FMEAs, reliability analysis, environmental qualification, and link them to the claims made in the safety demonstration. The BSC should identify the use of defensive design and fault revealing techniques. The BSC should identify the pedigree of any COTS and pre-developed components and		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

CIM – ADEQUACY OF SAFETY CASE

GI-AP1000-CI-09 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-09**	**GDA Issue Action Reference**	**GI-AP1000-CI-09.A2**
	provide a demonstration of the adequacy of the development arrangements. For older components the safety argument might involve use of proven in use arguments and testing rather than a production excellence argument. In either case any compensatory measures undertaken to address shortfalls should be identified in the safety demonstration. The BSC should demonstrate how the design and implementation of the equipment using complex / programmable, components, e.g. microprocessors, ASICs, and Field Programmable Gate Arrays complies with relevant WEC safety principles and standards. Given the programmable nature of such complex devices, the justification should draw on SAP ESS.27 a special case procedure for the demonstration of safety that involves the presentation of an argument of production excellence and implementation of independent confidence building measures. Where complex hardware is involved, the BSC should identify how the safety demonstration conforms to ESS.21 and the need for measures such as independent third party assessment. The BSC should include a plan that shows the forward activities, and production of related safety case documentation and evidence. Interim BSCs should be provided, particularly for large complex systems. A BSC for the completed design[1] should be submitted as soon as reasonably practicable before permission to commence nuclear site construction is sought. A BSC for installation and commissioning would be expected before equipment is delivered to site. Notes 1. Completed design – The design is complete at the point where the: • requirements, specifications, and implementation details (e.g. software coding and circuit diagrams etc.) have been completed; • production verification and validation activities (i.e. prior to delivery to site) have been completed; and • prototype equipment has been produced and subject to performance and qualification testing. With agreement from the Regulator this action may be completed by alternative means.		

Annex 2

WESTINGHOUSE AP1000® GENERIC DESIGN ASSESSMENT

GDA ISSUE

CLASS 1 DISPLAYS AND CONTROLS

GI-AP1000-CI-010 REVISION 0

Technical Area	**CONTROL AND INSTRUMENTATION**		
Related Technical Areas	None		
GDA Issue Reference	**GI-AP1000-CI-010**	**GDA Issue Action Reference**	**GI-AP1000-CI-10.A1**
GDA Issue	Westinghouse has advised that the protection and monitoring system (PMS) qualified data processing system (QDPS) and supporting AF100 bus will be upgraded to meet Class 1 requirements. This will facilitate the display of high integrity information in the MCR. ONR has sought to determine the provision of Class 1 displays and controls in the Remote Shutdown Room (RSR) and has been advised that there are none. Westinghouse is required to review the reasonable practicability of providing Class 1 displays and controls in the RSR.		
GDA Issue Action	The regulatory expectation is that Class 1 displays and controls are provided in an alternate emergency location (the RSR). In their absence, Westinghouse is required to: • Provide class 1 displays and controls in an alternative emergency location; or • Provide a justification of why the current design choice (of hardwired Class 2 manual control panels and Class 3 computer based controls and displays) is acceptable against the SAPs and Regulatory expectations. This should include an explanation, with a supporting justification, of why it is not reasonably practicable to provide Class 1 displays and controls in an alternative location. With agreement from the Regulator this action may be completed by alternative means.		

Annex 3

TSC Task Summary - GDA Step 4 C&I SAP Conformance Safety Case Maps and CAE Trail Review for AP1000[1]

Note this information has been imported from a TSC report (Ref. 51) and the formatting of the TSC report has been retained.

This Annex refers to the Pre-Construction Safety Report (PCSR) and European Design Control Document (DCD), which are references to the:

> AP1000 Pre-construction Safety Report, UKP-GW-GL-732 Revision 2, Westinghouse Electric Company LLC, December 2009, (Ref. 22); and
>
> AP1000 European Design Control Document, EPS-GW-GL-700 Revision 1, Westinghouse Electric Company LLC, December 2009, (Ref. 27);

respectively.

[1] Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 3

Annex: TSC Task Summary: C&I SAP Conformance and PCSR CAE Trail Review for AP1000

The aim of the Task 13 review has been to gain confidence that Westinghouse have adequate evidence to demonstrate that the claims and arguments presented in the Pre-Construction Safety Report (PCSR) and European Design Control Document (DCD) are adequately substantiated, and that the design of the C&I for the UK AP1000 can be shown to be in conformance with the HSE / ND C&I SAPs or that adequate justifications have been provided for any non-conformances.

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of C&I Safety Assessment Principles (SAP) conformance and PCSR Claims-Argument-Evidence (CAE) Trail (including review of Safety Case Maps (SCM)) for the UK AP1000 reactor design (TSC Task 11-13). NB. The SCM were provided by the Requesting Party (RP) to improve the demonstration of SAP conformance following review comments on the identified shortfalls in the original safety case documentation.

The Requesting Party (RP) for the UK AP1000 reactor design is Westinghouse Electric Company (WEC).

The main areas of activity covered in the Task 13 review were:

- the WEC demonstration of Conformance with the HSE / ND C&I SAPs;
- the safety case for selected sample Sensors;
- PCSR updates received during the period of the Step 3 (TSC Tasks 1 to 3), and
- Technical Observations raised by Step 3 Task 1 to 3 in relation to Claims and Arguments for conformance with HSE / ND C&I SAPs.

This Task 13 review follows on from the review of Claims and Argumentation in support of conformance with HSE / ND C&I SAPs carried out in preliminary Step 3 activities (TSC Tasks 1 to 3). The aim of Tasks 11 and 12 was to review the Claims and Arguments for those SAPs not addressed during Step 3. Tasks 11 and 12 were not progressed as separate tasks and the scope of these tasks was covered by the TSC Task 13 high level review of SCM. During Step 3, the first activity was a review of the compliance claim made in the SAP Compliance Roadmap UKP-GW-GL-710 Section C and the sections of the PCSR Revision 0 and DCD Revision 0 to which the Roadmap directs.

This review concluded that the SAP Compliance Roadmap was not precise enough to enable easy access to all the relevant information within the PCSR and DCD and recommended that this be improved. Westinghouse subsequently developed and issued SCM for each of the SAPs. The CAE Trail demonstration presented in the SCM was reviewed by the Step 4 TSC Task 13.

A total of 48 technical observations resulting from the review have been raised. These technical observations (TO) have been designated TO1 or TO2 by the TSC depending on their significance, of which TO1 is the higher – 2 of these have been designated TO1 and 46 have been designated TO2.

<u>SAP Conformance Claims-Arguments-Evidence Review</u>

Annex 3

The Westinghouse approach to demonstration of SAP conformance is to generate Safety Case Maps (SCM) for each SAP that link the HSE / ND C&I SAP requirements to Evidence documents identified by WEC as supporting claims and arguments for SAP conformance. The SCM, which have undergone a number of iterations during Step 4 with feedback from the TSC and HSE / ND have been used as the basis for the TSC Task 13 sampled evidence review. The overall aim of Task 13, and the main focus of this report, has been to arrive at an opinion on the level of conformance against the SAPs as demonstrated through the RP's CAE Trail, in this case presented via the SCM.

The 84 SAPs intended to be reviewed by Task 13 were divided into 4 Phases to prioritise the review process. Specific SAPs were apportioned to a number of other TSC Step 4 Tasks for sampled evidence review in the context of these Tasks.

An initial high level review of the submitted SCM for the 45 Phase 1 and Phase 2 SAPs was undertaken to determine the level of adequacy based on the coverage of SAP requirements, level of argument, relevance to applicable safety/safety-related systems, and appropriateness of the evidence identified by the RP.

This initial high level review of the CAE Trails in the SCM indicates that 38 of the 45 Phase 1 and Phase 2 SAP CAE Trails have significant areas for improvement (AFI). As most CAE Trails have a number of AFI a Step 4 technical observation (TO) (T13.TO1.01) has been raised to address these. T13.TO1.01 is supported by 45 further Step 4 technical observations (T13.TO2.01 to T13.TO2.45).

Due to the ongoing revision of WEC SCM it was only possible to commence the review of the SCM and the sampled review of evidence, towards the end of Step 4. In addition, with the results of the initial SCM review and importance of other high priority review work, and time left for review within the timeframe of GDA Step 4 it was agreed with HSE / ND to conduct a sample review of evidence against a limited sample of six HSE / ND C&I SAPs. A sample of supporting evidence against the SCM CAE Trails was reviewed for the following six SAPs selected for the sample:

ECS.3, EQU.1, ESR.5, ESS.21, ESS.27 and EDR.2

The sampled evidence review of the CAE Trails in the SCM for these six SAPs concluded that WEC has not demonstrated an 'acceptable' level of SAP conformance. The key generic areas for improvement are:

- Inappropriate reference to evidence.
- Lack of clear identification of evidence within a document.
- SCM do not address all appropriate systems and platforms.
- Clear 'Argument' not always apparent due to limited information in the 'Sub-claims'.
- Lack of revision control of identified evidence.
- Much of the evidence has not been made available and is identified in the SCM as 'LATER'. Such documents would need to be produced / reviewed by the designer or future operator / licensee.

Annex 3

- WEC apply IEEE standards and there needs to be clear reference to IEC standards as agreed with WEC as being appropriate and the demonstration of compliance to IEC standards produced as agreed with HSE / ND. However no clear identification of, or demonstration of compliance with, specific IEC Standards and Clauses (where appropriate) to support the argument has been presented.

In addition to the sampled review of evidence against the six SCM CAE Trails, further evidence document review work was carried out by TSC Tasks 14 to 18 in the context of relevant HSE / ND SAPs. The approach and discussion on the evidence review in the context of SAPs by Tasks 14 to 18 is covered in the respective TSC Task reports and associated Public Summaries. The SAPs covered by this evidence review are:

ECS.1, ECS.3, ECS.5, EQU.1, EDR.1, EDR.2, EDR.3, ESS.11, ESS.18, ESS.21, ESS.23, ESS.27, ESR.5, ERL.1, ERL.2 and ECM.1

A TO (T13.TO1.02) which has been raised to address these TSC Tasks 14 to 18 SAP evidence reviews is supported by 14 TOs raised by TSC Tasks 14 to 18 during the sample review of evidence against the CAE Trails in support of TSC Task 13. The specific context of the supporting TOs raised against the SCM is presented in a matrix *'NII GDA Technical Review – C&I - Step 4 Tasks UK AP1000 CAE Trail & Evidence Review Matrix, 37194/64263V Issue 1.0'*.

T13.TO1.02 is also supported by a further 51 TOs raised in the context of SAPs by TSC Tasks 14 to 18 in the course of safety case evidence review. The specific context of the TOs raised by Tasks 14 to 18 during their task review work is presented in the respective TSC Task reports and Public Summaries.

<u>Sensor Review Conclusions</u>

A review of Sensors (excluding Smart sensors that use microprocessors) used within the UK AP1000 C&I design was undertaken. This was intended to cover In-core, Ex-core and Process Instrumentation sensors/detectors. The Westinghouse GDA Scope for Instrumentation as stated in letter UN REG WEC 000206, dated 30 April 2010, appears limited to the In-core Instrumentation System (IIS) only with no reference to any Ex-core or Process Instrumentation. UN REG WEC 000206 defines the GDA scope for the IIS as:

- Design Requirements and System Definition – All evidence complete and available. However, UN REG WEC 000206 states that the IIS System Design Requirements (APP-IIS-J4-001) and IIS System Design Specification (APP-IIS-J7-001) will not be issued as a Rev. 0 for GDA; i.e. first formal issue. However, Rev A that has not been through the full WEC review process was provided in response to a technical query (TQ-AP1000-1174) in December 2010 and used in the review.

- Design, Implementation and Testing – Documentation specifying the processes will be available but not the output from the processes.

- Installation – Out of scope for GDA.

An initial review of the PCSR and DCD did not reveal sufficient information for this review of sensors. A technical query TQ (TQ-AP1000-1174) was raised by HSE / ND requesting information on IEC

Annex 3

standards used or required to be used in relation to sensors (In-core, Ex-core and Process) and demonstration of compliance with them. The TQ sought to illicit for such sensors:

- Which IEC Standards (or equivalent ~ equivalence to be stated) are applied or required of suppliers to apply;
- How conformance with these Standards is demonstrated;
- Details of the sensors where available (e.g. make, model, specification);
- Clarification of Categorisation and Classification.

The WEC response to TQ-AP1000-1174 identified a range of standards but the majority were not IEC standards and no equivalence information was provided. The TQ-AP1000-1174 response stated this would be provided in the future. Minimal conformance to IEC standards and sensor details were also provided.

WEC also stated that a compliance statement for IEC standards would be provided following receipt of an order for a UK AP1000. In lieu of this essential information, the TSC undertook a review of WEC documents against a sample IEC standard to provide an indication of the level of compliance. This considered the UK AP1000 In-core Instrumentation System (IIS) System Specification Document (SSD), APP-IIS-J7-001, Revision A against the first 42 requirements of BS IEC 60737:2010 (Nuclear Power Plants - Instrumentation Important to Safety - Temperature Sensors (in-core and primary coolant) - Characteristics and test methods). These 42 requirements cover approximately two thirds of the requirements in the standard and, in the TSC's opinion, would provide a representative indication of the level of compliance of the IIS design against the standard.

The IIS system specification (SSD) presents a broad range of functional and environmental requirements for the in-core instrumentation system, including the Core Exit Thermocouples (CETs). The requirements are generally presented at high level without justification for the requirements, their origin / derivation or why they are regarded as appropriate and correct. The SSD references limited evidence to demonstrate implementation of the requirements in the UK AP1000 design. Several appendices were included as placeholders with a comment indicating the content was to be provided at a later date. Four references were similarly identified. The review against 42 clauses of IEC 60737 found:

- Compliance with 5 clauses.
- Partial compliance with 12 clauses: Most of these were due to the need for supporting justification and evidence, although some statements only partially covered the issue raised in the standard.
- Non compliance with 25 clauses: Almost all non compliances were because the IIS System Specification did not include content directly addressing the issue identified by the clause in the standard. E.g.:
    - Use of mineral cables.
    - Avoidance of EMI on cable routes.

Annex 3

- No discussion on response time.
- No justification for shock and vibration data.
- No discussion on compatibility with other core materials.

Given the absence of an explanation of compliance with IEC standards, the low level of compliance found in the review and the limited evidence availability at this time, further review was not undertaken.

This review therefore concludes that all observations in TQ-AP1000-1174 remain to be satisfactorily addressed. Technical observation T13.TO2.46 has been raised to address these areas for improvement.

PCSR and DCD Update Impact Review

For the Westinghouse AP1000, the Step 3 reviews were carried out using the PCSR revision 0 and the DCD revision 0. Westinghouse then issued new revisions of both the PCSR and the DCD; the PCSR at revision 2 and the DCD at revision 1. The up-issued documents were reviewed against the earlier versions to understand whether there were any changes to the observations or conclusions identified in the Step 3 reviews.

The changes from PCSR revision 0 to PCSR revision 2 introduced significant restructuring; however, the system architecture and C & I text, specifically for the systems performing a safety-related role remained unchanged.

Additional information, drawn from the DCD, has been introduced into the C & I section of the PCSR revision 2, and additional references to either subsections of the PCSR, the DCD, the Defence in Depth report or the Safety Criteria for the AP1000 C & I System report had been included. Not all the PCSR subsection references for descriptions of the supporting duty systems for the PLS (section 6.7.3) are correct, in some cases the subsection reference was to a different system description or the section does not exist.

The up-issue of the PCSR from revision 0 to revision 2 did not include any significant changes in terms of the safety case structure, (including response to the SAPs); the specific claims on the systems and supporting argument and evidence trail was still not clear. There was a minor improvement in Section 6.7.2 of the PCSR to provide evidence for some specific claims made against a function of a safety-related C & I system.

The change control notice for the DCD states the document had been revised to include changes to the standard design that were a result of Westinghouse design finalisation reviews and changes committed to the US NRC resulting from their review. Although there had been minimal changes, specific modifications relate to determining reactor trip parameters and these were considered as part of the TSC Task 16 review.

Technical Observations

Task 13 has performed a review of a sample of WEC Safety Case Maps and In-Core Instrumentation sensors. Task 13 has raised a total of 48 technical observations resulting from this review; 2 of these

Annex 3

observations have been designated as TO1 (T13.TO1.01 and T13.TO1.02). However, 45 of these technical observations, designated TO2 (T13.TO2.01 to T13.TO2.45), have been raised by Task 13 that support the TO raised by Task 13 (T13.TO1.01) against the CAE Trail presented as the basis of the WEC demonstration of conformance with the HSE / ND C&I SAPs (i.e. Safety Case Maps). Additionally, 65 technical observations have been raised by TSC Step 4 Tasks 14 to 18 that support the TO raised by Task 13 (T13.TO1.02) against the sampled review of evidence from the CAE Trails that the RP claims support SAP conformance and further review of evidence against SAPs by TSC Step 4 Tasks 14 to 18 (see table appended to T13.TO1.02). These other Step 4 TSC Task observations are reported in the applicable Step 4 TSC Task reports. One observation has been designated as TO2 (T13.TO2.46) against Sensors (In-Core, Ex-Core and Process).

Technical Observations designated TO1:

T13.TO1.01 – A high level review of 45 Phase 1 and Phase 2 Safety Case Maps (SCM) issued by WEC for the demonstration of conformance to the HSE / ND C&I SAPs have been reviewed and it was found that there are significant areas for improvement (AFI) in the presented Argument and identified Evidence for these SAPs. The AFI relating to the CAE Trails for HSE / ND C&I SAPs are addressed in 45 Technical Observations (TO) (T13.TO2.01 to T13.TO2.45). The designer or future operator / licensee is requested to produce adequate SCM for the 84 HSE / ND C&I SAPs taking into account all AFI in the 45 supporting TOs in further development of a robust demonstration of conformance with the HSE / ND C&I SAPs.

T13.TO1.02 – Following sampled evidence review against a sample of six Safety Case Maps (SCM) CAE Trails issued by WEC for the demonstration of conformance to the HSE / ND C&I SAPs and further review of evidence against SAPs by Tasks 14 to 18, TSC Step 4 Tasks 14 to 18 identified areas for improvement (AFI) and raised 65 TOs, as listed in the Table below, that are reported in detail in the respective Task reports. The designer or future operator / licensee is requested to take all AFI in these TO raised by TSC Tasks 14 to 18 into account in further development of a robust demonstration of conformance with HSE / ND C&I SAPs.

SAP	Title	Task 14	Task 15	Task 16	Task 17	Task 18
TOs raised by TSC Tasks 14-18 during sampled review of evidence against SCM i.e WEC's SAP conformance demonstration						
ECS.3	Standards.	T14.TO2.03				
EQU.1	Qualification procedures.		T15.TO2.49	T16.TO2.44		
EDR.2	Redundancy, diversity and segregation.		T15.TO2.47	T16.TO2.30	T17.TO2.03	T18.TO2.11
ESS.21	Reliability.		T15.TO2.50	T16.TO2.40	T17.TO2.04	
ESS.27	Computer based safety systems.		T15.TO2.51	T16.TO2.29		
ESR.5	Standards for computer based equipment.		T15.TO2.48	T16.TO2.39		
TOs raised by TSC Tasks 14-18 during evidence review in the context of the tasks and relevant sampled SAPs						
ECS.1	Safety categorisation and standards.		T15.TO2.19			

Annex 3

ECS.3	Standards.		T15.T02.10 T15.T02.54			
ECS.5	Use of experience, tests or analysis.		T15.T02.03 T15.T02.21			
EQU.1	Qualification procedures.		T15.T02.04 T15.T02.22 T15.T02.30 T15.T02.57 T15.T02.58 T15.T02.59	T16.T02.15		
EDR.1	Failure to safety.		T15.T02.24 T15.T02.25	T16.T02.09 T16.T02.45		
EDR.2	Redundancy, diversity and segregation.		T15.T02.23 T15.T02.57 T15.T02.59	T16.T02.07 T16.T02.15 T16.T02.22	T17.T01.01 T17.T02.01	T18.T02.19 T18.T02.20 T18.T02.21 T18.T02.24 T18.T02.25
EDR.3	Common cause failure.			T16.T02.25	T17.T01.01 T17.T02.02	T18.T02.06 T18.T02.12
EDR.4	Single failure criterion			T16.T02.15		
ESS.1	Requirement for safety systems			T16.T02.15		
ESS.2	Determination of safety system requirements			T16.T02.15		
ESS.3	Monitoring of plant safety				T17.T01.02	
ESS.7	Diversity in the detection of fault sequences			T16.T02.15		
ESS.8	Automatic initiation				T17.T01.02	
ESS.11	Demonstration of adequacy.		T15.T02.32			
ESS.18	Automatic initiation.				T17.T02.02	
ESS.21	Reliability.		T15.T01.06 T15.T02.25 T15.T02.26 T15.T02.27 T15.T02.57 T15.T02.58 T15.T02.59	T16.T02.01 T16.T02.07 T16.T02.05 T16.T02.15		

Annex 3

			T15.T02.61 T15.T02.63			
ESS.22	Avoidance of spurious operation			T16.T02.15		
ESS.23	Allowance for unavailability of equipment.				T17.T02.01	
ESS.27	Computer based safety systems.		T15.T02.01 T15.T02.11 T15.T02.12 T15.T02.15 T15.T02.22 T15.T02.27 T15.T02.40 T15.T02.57 T15.T02.58	T16.T02.01 T16.T02.22		
ESR.3	Provision of controls			T16.T02.15 T16.T02.22		
ESR.5	Standards for computer based equipment.		T15.T02.14 T15.T02.46	T16.T02.01 T16.T02.10		
ESR.9	Response of control systems to normal plant disturbances			T16.T02.22		
ERL.1	Form of claims.		T15.T02.61			
ERL.2	Measures to achieve reliability.		T15.T02.61			
ECM.1	Commission testing		T15.T02.20	T16.T02.32		
EHF.8	Personnel competence		T15.T02.67			
EMT.7	Functional testing			T16.T02.15 T16.T02.17 T16.T02.22		

Technical Observation designated TO2:

T13.T02.01 - From the review of the CAE Trail presented in the SCM for ECS.1 the following areas for improvement are raised:

- On both sheet 1 and 2 of the SCM, there is a stand-alone claim (a green rectangular box) that indicates that the WEC (US) classification processes comply with IEC 61226. WEC would be expected to claim that the UK documents ensure compliance with IEC 61226, or identify evidence to demonstrate US process compliance with IEC 61226, but this is not evident. Furthermore it is not clear why this claim is not part of the main SCM structure. The designer or future operator / licensee is requested to produce a demonstration of compliance to IEC 61226 and to ensure this is clearly identified in the SCM.

Annex 3

- SAP Guidance Para 150 is only partly covered - it is not clear how all of parts a) to d) are fully captured by the SCM. The designer or future operator / licensee is requested to produce a SCM which covers all aspects of the SAP.

- Generally there is a lack of logical progression from the top claim to the sub-claims. The designer or future operator / licensee is requested to review the SCM and produce a revision to ensure a logical progression of the argument.

- Evidence documents do not refer to specific sections. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified as appropriate.

T13.T02.02 - From the review of the CAE Trail presented in the SCM for ECS.2 the following areas for improvement are raised:

- There is a stand-alone claim (a green rectangular box) indicates that the WEC (US) classification processes comply with IEC 61226. It would have been expected WEC to claim that the UKP documents ensure compliance with IEC 61226 but this is not evident. Furthermore it is not clear why is this not part of the main SCM structure. The designer or future operator / licensee is requested to produce a revised SCM which clearly identifies an adequate demonstration of compliance to IEC 61226 .

- SCM requires clearer claims w.r.t. each part of the SAP and to point to specific sections in documents UKP-GW-GL-044 & 144 where evidence is located. Claim corresponding to SAP Para 153 (use of deterministic / probabilistic methods) is not evident. Although claims corresponding to guidance Paras 155 and 156 are present there is no supporting CAE trail. The designer or future operator / licensee is requested to ensure that the SCM covers all aspects of the SAP.

- Evidence document references do not identify specific sections. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.03 - From the review of the CAE Trail presented in the SCM for ECS.3 the following areas for improvement are raised:

- The SCM should cover the complete (or essential points of the) SAP paragraph. The designer or future operator / licensee is requested to produce an update to the SCM covering all aspects of the SAP.

- The SCM should adequately address the intent of the SAP (para 158 in particular) - to identify the standards (i.e. IEC) that WEC claim compliance with, and for what I&C system. The designer or future operator / licensee is requested to produce an update to the SCM that identifies all IEC standards to which compliance is claimed.

- Para 159 - It is not clear if WEC have evaluated the standards/codes for their applicability. NB the current wording in node ECS.3.2.4 is not relevant to para 159 but is useful to the overall SAP. The designer or future operator / licensee is requested to produce an update the SCM to provide a clear demonstration of the applicability of standards and codes.

Annex 3

- Para 160 - It is not clear if WEC are claiming independence between multiple safety functions, and if so, how this is justified. The designer or future operator / licensee is requested to produce an update to the SCM which clearly addresses independence between multiple safety functions or, if not claimed, produce a clear justification for acceptability.

- Evidence documents do not always refer to specific sections. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.04 - From the review of the CAE Trail presented in the SCM for EQU.1 the following areas for improvement are raised:

- There is no sub-claim to guidance para 163 (see below node EQU1.2), the SAP para is linked directly to evidence. There is no sub-claim that there is a 'physical demonstration' as required by guidance para 164 (see below node EQU1.3). There is no separate sub-claim for the main SAP wording in node EQU.1. The designer or future operator / licensee is requested to produce an update to the SCM covering all aspects of the SAP.

- No specific AP1000 I&C systems are cited although it is inferred that the SCM applies to all I&C systems. The designer or future operator / licensee is requested to produce an update to the SCM that clearly identifies and covers all applicable systems and platforms.

- Evidence documents do not always refer to specific sections. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.05 - From the review of the CAE Trail presented in the SCM for EDR.1 the following areas for improvement are raised:

- Node EDR1.2.1 - there should be a clear sub-claim that the PMS was "*designed to be inherently safe or fail in a safe manner*" that may still point to the same evidence as node EDR1.2.1.7. This would confirm that nodes EDR1.2.1.1 to 1.2.1.6 cover the full scope of PMS. The designer or future operator / licensee is requested to produce an update to the SCM that includes a clear claim that the PMS in designed to fail in a safe manner.

- Not clear that systems have been "designed to be inherently safe and/or fail-safe" in operation (current EDR1.2 claim is that they "fail in a safe manner"). The claim at node 1.2.1.1 is for failure to preferred failure states not for inherently safe / fail safe; the claim at node 1.2.1.3 is for default to a predefined value not for inherently safe / fail safe. There is a claim that all PMS faults detected by the self diagnostics are fail safe at 1.2.1.5; it is unclear how this is consistent with the claims above and with the behaviour required of the ESF components. The designer or future operator / licensee is requested to produce an update to the SCM that includes a clear demonstration that safety systems are designed to be inherently safe / fail safe.

- Node EDR1.2.2 - DAS does not appear to be fail-safe - WEC state that the DAS is an 'energise to actuate' system. For the DDS and DAS, sub-claims do not support node EDR1.2 claim for fail-safe. The designer or future operator / licensee is requested to produce an update to the

Annex 3

SCM that includes a clear demonstration that the DDS and DAS are designed to be fail-safe or provide appropriate justification of any non conformance.

T13.T02.06 - From the review of the CAE Trail presented in the SCM for EDR.2 the following areas for improvement are raised:

- 1) EDR2.1 - It is not clear how the diversity requirements were developed for each system, nor how diversity is incorporated for each system or between systems.
  2) EDR2.2 - It is not clear how the redundancy requirements were developed for each system, nor is it clear where and how redundancy is incorporated for each system or between systems.
  3) EDR2.3 - It is not clear how the segregation requirements were developed for each system, nor is it clear where and how segregation is incorporated for each system or between systems.
  4) EDR2.2.1 Not clear if DAS has internal redundancy.

  The designer or future operator / licensee is requested to produce an update to the SCM that provides clear demonstration of the application of diversity, redundancy and segregation.

- The references do not always point to specific chapters / sections of the documents. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.07 - From the review of the CAE Trail presented in the SCM for EDR.3 the following areas for improvement are raised:

- 1) EDR.3.3 - No sub-claim for segregation;
  2) No IEC standards are claimed (but NUREG CR6303 is);
  3) No claim for redundancy made.
  4) Para 174 - No claim for two independent safety measures.
  5) EDR.3.2 - only has claim for S/W CCF rate.

  The designer or future operator / licensee is requested to produce an update to the SCM that addresses points 1-5.

- Few reference documents have section numbers cited. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.08 - From the review of the CAE Trail presented in the SCM for EDR.4 the following areas for improvement are raised:

- It is not clear how the Single Failure Criterion (SFC) applies to each "permissible state of plant availability" for each safety group as required by the SAP. The designer or future operator / licensee is requested to produce an update to the SCM that clearly demonstrates the application of SFC.

- It is not clear how the sub-nodes under EDR4.1.7 (SAP para 175) support the CAE trail for this node "consequential failure are integral to single failures" (only node EDR4.1.7.7 appears to be relevant). The designer or future operator / licensee is requested to produce an update to the SCM that fully addresses consequential failures.

Annex 3

- EDR4.1.1 - IEEE standards are cited, it is not clear how these support the SAP and if there are equivalent IEC standards that are applicable. The designer or future operator / licensee is requested to produce an update to the SCM that includes applicable IEC Standards and explains how the standards address the SAP requirement.

- Few reference documents have section numbers cited. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.09 - From the review of the CAE Trail presented in the SCM for ERL.3 the following areas for improvement are raised:

- Node ERL3.1 does not state which systems provide the automatic and reliable response - e.g. there are PMS documents that describe what ESFAS functions there are and how they are selected. The designer or future operator / licensee is requested to produce an update to the SCM that clearly identifies the Safety Systems provided for automatic and reliable response.

- Node ERL.3.2 does not support para 180 and TSC would expect this node to link to (support) the main SAP wording. The designer or future operator / licensee is requested to produce an update to the SCM covering all aspects of the SAP.

- It is not clear how the decision between automatic or manual initiation has been made, e.g. required time response and/or reliability considerations. The designer or future operator / licensee is requested to produce an update to the SCM that includes a clear demonstration of process for deciding between automatic and manual initiation.

- Not clear if there are functions that WEC claim manual intervention for e.g. longer timescale actions and if so what these are (node ERL.3.3 implies there are manual functions but does not state what they are). The designer or future operator / licensee is requested to produce an update to the SCM that clearly identifies the functions where manual initiation is required.

- Few reference documents have section numbers cited. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.10 - From the review of the CAE Trail presented in the SCM for EMT.7 the following areas for improvement are raised:

- There is no separate sub-claim to 'prove the complete system and safety related function of each component' (although some other claims do cover some related aspects). The designer or future operator / licensee is requested to produce an update to the SCM that clearly demonstrates that testing proves the complete system and safety related function.

- Although PMS, DAS and PLS are included under node EMT7.2, it is not clear if it is being claimed that 'complete functional testing' of these systems is not 'reasonably practicable' and what equivalent means of functional proving is being claimed. The designer or future operator / licensee is requested to produce an update to the SCM that clearly identifies systems for which 'complete functional testing' is not 'reasonably practicable' and the equivalent means of functional proving adopted.

Annex 3

- Claim made that testing does not actuate the DAS whereas the SAP requires 'no loss of safety function' - the claim is not clear. The designer or future operator / licensee is requested to produce an update to the SCM that clearly demonstrates that testing does not result in a loss of safety function.

- Not clear if functional testing is not reasonably practicable i.a.w. SAP Para 193. The designer or future operator / licensee is requested to produce an update to the SCM that clearly identifies where functional testing is not reasonably practicable.

- Claim made that maintenance of a DAS channel leaves only manual control - not clear how WEC justify the loss of automatic initiation. The designer or future operator / licensee is requested to produce an update to the SCM that demonstrates the acceptability of loss of automatic initiation by the DAS during testing.

T13.T02.11 - From the review of the CAE Trail presented in the SCM for ESS.1 the following areas for improvement are raised:

- CAE refers to shutdown (node ESS1.2.4), however the SAP requires a "defined safe state" and thus it is not clear whether WEC wish to claim that the only "defined safe state" is shutdown or whether ESFAS also needs to be included in the SCM. The designer or future operator / licensee is requested to produce an update to the SCM that clearly identifies all define safe states.

- There are missing claims for achieving and maintaining a defined safe state in "normal and fault conditions" as well as how the I&C relates to "margin of reactivity". The designer or future operator / licensee is requested to produce an update to the SCM covering all aspects of the SAP.

- Few reference documents have section numbers cited. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.12 - From the review of the CAE Trail presented in the SCM for ESS.2 the following areas for improvement are raised:

- There is no claim / argument for "..extent of SS provision, their functions, levels of protection...". Paragraph 337 is not fully covered since there is no explicit sub-claim for determining the "SS provisions, functions and required reliabilities". There is no explanation as to how defence in depth and reliability were determined - only "project documents" are referred to. The designer or future operator / licensee is requested to produce an update to the SCM covering all aspects of the SAP.

- The evidence documents do not always support the claims. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.13 - From the review of the CAE Trail presented in the SCM for ESS.3 the following areas for improvement are raised:

Annex 3

- 1) Not clear which systems provide monitoring and controls and what class are these systems. What is the scope of each and which stations (MCR / RSS) receive display data from these systems.

  2) There is no claim for monitoring plant state (only 'accident monitoring instrumentation')

  3) Node ESS3.3 simply states '*Safety Classification - Category B*' with no supporting argument. Guidance paragraph 338 requires '*Monitoring provisions should be classified as safety or safety-related systems as appropriate*'. It is unclear what the Classification of each monitoring provision is or why this node mixes Category and Class.

  4) SCM is not clear about the specification of monitoring provisions made and why they are adequate.

  The designer or future operator / licensee is requested to produce an update to the SCM covering all aspects of the SAP.

- Few reference documents have section numbers cited. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.14 - From the review of the CAE Trail presented in the SCM for ESS.7 the following areas for improvement are raised:

- 1) Not clear how diversity is achieved in SS initiation given that DAS only provides a sub-set of PMS functions. Issue of adequacy of diversity across PMS and DAS is being addressed by HSE.

  2) ESS7.2 - Monitoring variable diversity - the argument requires more detail, e.g. need clarification e.g. do the PMS and DAS use the same (but diverse) variables or if the PMS and DAS use different variables to achieve diversity (there are no arguments to link the claims to the evidence).

  The designer or future operator / licensee is requested to produce an update to the SCM that clearly demonstrates how diversity is implemented for monitoring, detection and initiation of Cat protection functions.

- Few reference documents have section numbers cited. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.15 - From the review of the CAE Trail presented in the SCM for ESS.8 the following areas for improvement are raised:

- Generally the CIM control needs clarification. e.g. Node ESS8.5 states "CIM local control can negate SS actions" - it is not clear if this can result from operator action in one cabinet or requires an interlock over-ride to gain access to other cabinets. Not clear if alarm relates to CIM as well as cabinet intrusion. Further clarification required in SCM as to why manual override of CIM is desirable. The designer or future operator / licensee is requested to produce an update to the SCM that fully addresses the CIM control functions.

Annex 3

- Node ESS8.4.1 refers to a IEEE 603 requirement for manual actuation and this is applied to the PMS (ESS8.4.1.1), however there is no trail evident for the DAS (ESS8.4.2). The designer or future operator / licensee is requested to produce an update to the SCM that includes requirements for manual actuation of the DAS

- Few reference documents have section numbers cited. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.16 - From the review of the CAE Trail presented in the SCM for ESS.18 the following areas for improvement are raised:

- Nodes ESS18.3.1 - It is not clear how faults in "associated systems" do not affect SS by relying on the Single Failure Criterion (SFC) - TSC would expect system independence, segregation etc similar to that detailed below Node ESS18.1.1. The designer or future operator / licensee is requested to produce an update to the SCM that clearly demonstrates that safety systems are not affected by faults in 'associated systems'.

- Node ESS18.4 and below - There is no clear argument that the PMS and DAS withstand the identified hazards. The designer or future operator / licensee is requested to produce an update to the SCM that includes a clear demonstration of the PMS and DAS hazard withstand (e.g. by identifying appropriate evidence documents).

- Few reference documents have section numbers cited. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.17 - From the review of the CAE Trail presented in the SCM for ESS.21the following areas for improvement are raised:

- 1) WEC state para 355 is not relevant, however CIM (and possibly the new DAS) does use complex H/W.

  2) The wording of SAP ESS.21 is not always reflected in the claims / sub-claims.

  3) Some sub-claims do not appear relevant to the SAP intent - e.g. ESS.21.3.2.2 and ESS21.3.2.2.1 leading to sheets ('sub-maps') ESS.21B and ESS.21C. ESS21.3.1.2 to 4 do not appear to be relevant.

  4) No clear argument regarding how complexity was avoided (ESS21.1).

  5) ESS21.3.1 contains 3 nodes with no I&C relevance to fail safe approach.

  6) ESS21.4 is mainly about periodic testing, however no direct reference is made to SAP para 356.

  The designer or future operator / licensee is requested to produce an update to the SCM covering all aspects of the SAP.

Annex 3

- Few reference documents have section numbers cited. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.18 - From the review of the CAE Trail presented in the SCM for ESS.23 the following areas for improvement are raised:

- 1) No clear claim for the main SAP wording - i.e. how the SS was specified / designed to account for unavailability.

  2) Node ESS23.1.1 - it is not clear what "GDC 21" is and how this relates to this SAP.

  3) It is not clear how availability is maintained with respect to non-repairable failures (Node ESS23.1.4.1) and unrevealed failures (ESS23.1.4.2).

  The designer or future operator / licensee is requested to produce an update to the SCM covering all aspects of the SAP.

- Not many reference documents have section numbers cited. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.19 - From the review of the CAE Trail presented in the SCM for ESS.27 the following areas for improvement are raised:

- 1) Improve the CAE in particular w.r.t production excellence, especially Standards.
  2) Node ESS27.1.1.3 - there is no indication of the international standard(s) claimed.
  3) Node ESS27.3.4 - the sub-claims appear to relate to production excellence and not confidence building (sub-claims are identical to those used in confidence building).
  4) Node ESS27.2 - states "no weaknesses in production process", however the production process is not completed, thus the status of this claim is unclear.
  5) Other gaps/omissions are:- Production excellence and gaps cf. a) 880 work; b) IEC 60880 to IEC 880; c) Addressing gaps through compensating activities. d) software version numbers for platform components.

  The designer or future operator / licensee is requested to produce an update to the SCM covering all aspects of the SAP.

- Not all reference documents have section numbers cited. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.20 - From the review of the CAE Trail presented in the SCM for ESR.1 the following areas for improvement are raised:

- 1) Sub-claim ESR.1.1 appears to be superfluous - furthermore it is not clear how the top-claim requirement for central and remote control locations are captured in the sub-claims.
  2) Sub-claims to para 366-1 (node ESR.1.1.2) - There is no clear statement for what systems are sited in each location and how they apply to normal ops, fault conditions and severe

Annex 3

accidents - the current structure is overly complex (19 sub-claims). 3) For sub-claim ESR.1.1.2.3 there are no sub-claims to support it, whereas the first sentence to para 366 has many sub-claims.

The designer or future operator / licensee is requested to produce an update to the SCM covering all aspects of the SAP.

- Not all reference documents have section numbers cited. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.21 - From the review of the CAE Trail presented in the SCM for ESR.3 the following areas for improvement are raised:

- Not clear what controls are available based on the top claim and how they maintain variables within specified ranges. The designer or future operator / licensee is requested to produce an update to the SCM that clearly identifies the appropriate controls and how they maintain variables within specific ranges.

- Node ESR3.1 claims adequacy through compliance with regulatory codes/guidance and standards but does not state which ones. It is not clear how the controls are justified as adequate based on requirements. Currently adequacy is claimed by stating that the US reg. guides have been followed and thus it is not clear how this ensures SAP compliance. The designer or future operator / licensee is requested to produce an update to the SCM that clearly identifies applicable codes and standards, and the justification of the adequacy of the controls provided (e.g. including analysis of control lop stability and robustness etc).

- Not all reference documents have section numbers cited. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.22 - From the review of the CAE Trail presented in the SCM for ESR.5 the following areas for improvement are raised:

- The claims / arguments do not state the applicable hardware / software classes and thus why the corresponding standards are used (e.g. it is not clear whether IEC 60987 - which is applicable to Class 1/2 hardware - is used for AP1000 Class 3 I&C). The designer or future operator / licensee is requested to produce an update to the SCM that identifies applicable IEC standards or standards that have been demonstrated to be equivalent to the IEC standards corresponding to the Safety System Class.

- Not all reference documents have section numbers cited. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.23 - From the review of the CAE Trail presented in the SCM for ESR.7 the following area for improvement israised:

Annex 3

- Several types of communication system are listed, however it is not clear what they do and also why they are considered adequate. There is no clear claim the Safety Systems (SS) or Safety Related Systems (SRS) will be unaffected by the communication systems listed. The designer or future operator / licensee is requested to produce an update to the SCM that clearly identifies appropriate and adequate communications systems and the effect they have on the SS and SRS. NB. This can be provided by reference to sections of the PCSR / DCD and other identified evidence documents.

T13.T02.24 - From the review of the CAE Trail presented in the SCM for ERC.2 the following areas for improvement are raised:

- Node ERC2.1.1.2.2 - Not clear which protection system(s) can initiate boron injection. The designer or future operator / licensee is requested to produce an update to the SCM that clearly identifies the system(s) responsible for initiating boron injection and demonstrates independence and diversity from the system initiating reactor trip via the rods.

- Not all reference documents have section numbers cited. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.25 - From the review of the CAE Trail presented in the SCM for ERL.1 the following areas for improvement are raised:

- 1) SAP guidance Para 178 is not covered by SCM.
  2) I&C systems do not have specific claims made w.r.t. adequacy, or otherwise, of the reliability claims.
  3) There should be more detailed sub-claims that provide a link to the evidence documents.

  The designer or future operator / licensee is requested to produce an update to the SCM covering all aspects of the SAP.

- Reference documents do not have section numbers cited. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.26 - From the review of the CAE Trail presented in the SCM for ERL.2 the following areas for improvement are raised:

- 1) There is a requirement that the 'assumptions made in the course of reliability analysis' (from para 178) are stated, however, this is not addressed by the sub-nodes below ERL2.2. There needs to be an argument that specifically identifies how and where assumptions are addressed.
  2) Random and systematic analyses are not considered (para 178).
  3) More details / specific examples re. 'Quality Assurance' need to be provided (Node ERL.2.2.1).
  4) More detailed argument that separates out claims for the systems (e.g. PMS, DAS, PLS), hardware / software aspects and random / systematic failures (Node ERL.2.2.3) is needed.

Annex 3

The designer or future operator / licensee is requested to produce an update to the SCM covering all aspects of the SAP.

T13.T02.27 - From the review of the CAE Trail presented in the SCM for EMT.1 the following areas for improvement are raised:

- 1) The claims only relate to 'Safety Systems' and do not include SRS (PLS) (Nodes EMT.1.1 to 1.3).
  2) More is detail is needed in the sub-claims e.g. specify what drives the testing, maintenance and inspection requirements (reliability targets?).

  The designer or future operator / licensee is requested to produce an update to the SCM covering all aspects of the SAP.

- Some reference documents do not have section numbers cited. Lack of evidence relating to the DAS and PLS systems. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.28 - From the review of the CAE Trail presented in the SCM for EMT.3 the following area for improvement is raised:

- No explicit claim that all I&C systems are covered by the claims. The designer or future operator / licensee is requested to produce an update to the SCM that clearly identifies all applicable C&I systems.

T13.T02.29 - From the review of the CAE Trail presented in the SCM for EMT.6 the following areas for improvement are raised:

- 1) The claims made relate to SS (PMS and DAS) and do not include SRS (PLS) (Nodes EMT.6.1.1 to 6.1.4 state 'safety systems').
  2) Need more detail in the sub-claims to give examples of what 'provisions' to support testing/maintenance etc are to be provided for I&C systems and why they are appropriate and adequate.

  The designer or future operator / licensee is requested to produce an update to the SCM covering all aspects of the SAP.

- Some reference documents do not have section numbers cited. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.30 - From the review of the CAE Trail presented in the SCM for ELO.2 the following areas for improvement are raised:

- Control of key / key switches not covered. The designer or future operator / licensee is requested to produce an update to the SCM that addresses control of keys and key switches.

- No sections cited in reference documents. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

Annex 3

T13.T02.31 - From the review of the CAE Trail presented in the SCM for EHA.1 the following area for improvement is raised:

- No mention of EMI shielding (rooms, enclosures). No clear indication of how internal and external EMI sources will be identified. The designer or future operator / licensee is requested to produce an update to the SCM that identifies all EMI sources and how they are protected against.

T13.T02.32 - From the review of the CAE Trail presented in the SCM for ESS.9 the following areas for improvement are raised:

- DAS manual actuations - no sub-claims for this aspect. The designer or future operator / licensee is requested to produce an update to the SCM that covers DAS manual actuation.

- No justification for the stated intervention times has been provided. The designer or future operator / licensee is requested to produce an update to the SCM that identifies the justification for stated intervention times.

T13.T02.33 - From the review of the CAE Trail presented in the SCM for ESS.10 the following areas for improvement are raised:

- PMS and DAS are not covered in the claims / arguments. The designer or future operator / licensee is requested to produce an update to the SCM that covers all applicable systems and platforms.

- 'Degradation mechanisms' is not dealt with by sub-claims (see node ESS.10.1.2.1). The designer or future operator / licensee is requested to produce an update to the SCM that addresses degradation mechanisms.

- The sub-claims (i.e. ESS.10.1.1.1 and 10.1.2.1) do not contain sufficient detail regarding the aspects of capability that have been covered. The designer or future operator / licensee is requested to produce an update to the SCM that contains sufficient detail to demonstrate that the claimed capability has been addressed.

- Some reference documents do not have section numbers cited. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.34 - From the review of the CAE Trail presented in the SCM for ESS.11 the following areas for improvement are raised:

- PMS and DAS are not covered in the claims / arguments, although evidence does cover I&C systems. The designer or future operator / licensee is requested to ensure that the SCM covers all applicable systems.

- Not clear how SS adequacy is demonstrated by the functional requirements specification, Defence in Depth, PRA, reliability etc. (Node ESS.11.1.1). The designer or future operator / licensee is requested to produce an update to the SCM that clearly identifies how the cited

Annex 3

evidence demonstrates SS adequacy, i.e. of the system design as a means of achieving the specified function and reliability.

- Node ESS.11.2.1.1 refers to SRS (not relevant to this ESS SAP), in any case the intent of this sub-claim is unclear. The designer or future operator / licensee is requested to produce an update to the SCM covering all aspects of the SAP.

- Some reference documents do not have section numbers cited. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.35 - From the review of the CAE Trail presented in the SCM for ESS.12 the following areas for improvement are raised:

- Sub-claims do not address the main intent of the SAP - how does the design prevent the removal of services (e.g. power) that support SS, or if reduced to a sufficiently low likelihood that there is a fail safe outcome. Not clear that analyses are claimed to show this. The designer or future operator / licensee is requested to produce an update to the SCM covering all aspects of the SAP.

- Some reference documents do not have section numbers cited. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.36 - From the review of the CAE Trail presented in the SCM for ESS.13 the following areas for improvement are raised:

- Guidance para 349 not included in SCM. The designer or future operator / licensee is requested to produce an update to the SCM covering all aspects of the SAP.

- Not clear that operator will receive confirmation that all limiting conditions for which SS is qualified have been exceeded. The designer or future operator / licensee is requested to produce an update to the SCM that clearly identifies all applicable information received by the operator.

T13.T02.37 - From the review of the CAE Trail presented in the SCM for ESS.14 the following area for improvement is raised:

- References need section numbers. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.38 - From the review of the CAE Trail presented in the SCM for ESS.15 the following areas for improvement are raised:

- Not obvious from the claims what are MTP and ASU interfaces. The designer or future operator / licensee is requested to produce an update to the SCM that clearly identifies the MTP and ASU interfaces.

- References need section numbers. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

Annex 3

T13.T02.39 - From the review of the CAE Trail presented in the SCM for ESS.16 the following areas for improvement are raised:

- Not clear that the PMS and / or DAS are being considered (they are not named). The designer or future operator / licensee is requested to produce an update to the SCM that covers all applicable systems.

- Sub-claims do not explain how the PMS and DAS are independent of external energy supplies - furthermore it is not clear if they rely on their own dedicated sources. 'Safety DC and UPS' - not clear whether or not these are part of the SS (Sub-claim ESS.16.2). 'Ancillary ac generator' – it is not clear whether or not this is part of the SS (sub-claim ESS.16.3). The designer or future operator / licensee is requested to produce an update to the SCM that clearly addresses the independence of the PMS and DAS power supplies.

- References need section numbers. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.40 - From the review of the CAE Trail presented in the SCM for ESS.19 the following areas for improvement are raised:

- Sub-claims to node ESS.19.1 - WEC do not make an explicit claim that PMS / DAS are dedicated to only a single (safety) task of performing its safety function (there only appears to be an inference that this is the case). The designer or future operator / licensee is requested to produce an update to the SCM that clearly identifies whether the PMS and DAS are dedicated to a single safety function task of performing its safety function.

- References need section numbers. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.41 - From the review of the CAE Trail presented in the SCM for ESS.20 the following areas for improvement are raised:

- SAP requires that WEC shall identify any connections between safety systems and other C&I systems and if there are that they are:

    - unidirectional - out of the SS (e.g. monitoring only) and

    - that there are no faults associated with these other systems that could affect the SS.

  Currently the WEC sub-claims (ESS.20.1 and 20.1) only state "no direct connections" thus it is unclear what is being claimed. The designer or future operator / licensee is requested to produce an update to the SCM that clearly identifies connections between safety systems and other C&I systems and that they meet the requirements stated above.

- References need section numbers. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.42 - From the review of the CAE Trail presented in the SCM for ESS.24 the following areas for improvement are raised:

Annex 3

- No claim that minimum equipment will be defined by Tech Specs and that Tech Specs will be written to satisfy guidance documents. The sub-claims / arguments contain no detail that the SFC will be met. It is not clear how SFC is satisfied by 'defence in depth' and there is an implied claim that the SAP is met by a list of evidence documents (Node ESS.24.1.2). The designer or future operator / licensee is requested to produce an update to the SCM that clearly identifies how and where minimum equipment requirements are addressed and how the SFC will be met.

- The applicable I&C systems are not mentioned in the claims / arguments (they are in the evidence documents). The designer or future operator / licensee is requested to produce an update to the SCM that clearly identifies all applicable C&I systems.

- Some references need section numbers. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.43 - From the review of the CAE Trail presented in the SCM for ESR.4 the following areas for improvement are raised:

- Sub-claim re. 'operator indications and controls' (ESR.4.2) does not follow the SAP intent, the SAP requires the minimum safety-related I&C permitted to be substantiated. 'Industry standards' are claimed but none are cited. The designer or future operator / licensee is requested to produce an update to the SCM covering all aspects of the SAP.

- The applicable I&C systems are not mentioned in the claims / arguments (they are in the evidence documents). The designer or future operator / licensee is requested to produce an update to the SCM that clearly identifies all applicable C&I systems.

- References need section numbers. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13.T02.44 - From the review of the CAE Trail presented in the SCM for EKP.3 the following areas for improvement are raised:

- 1) Although references to control, monitoring, alarms, actuation, and post-accident instrumentation etc are made, it is not clear what I&C systems are being claimed (i.e. no reference to PLS, DAS and PMS).
  2) General Defence in Depth (DiD) strategy (Node EKP.3.1.1 / para 140) is only supported by a sub-claim that states DAS provides DiD as a back-up to the PMS. However this only corresponds to 'level 3' DiD and is more applicable to para 143 (table 1). A more robust argument should be provided on the application of DiD in support of sub-claim EKP.3.1.
  3) Fail-safe (Node EKP.3.6 / para 142-c) it is not clear what I&C systems have a fail-safe design.
  4) Severe accidents (Node EKP.3.7 / para 142-d) it is not clear what 'additional measures' are being claimed.
  5) DiD level 3 (as defined in the SAP Table 1) (Node EKP.3.8.3.1) it would be better to have separate sub-claims for nodes EKP.3.8.3 and 3.8.4 since level 3 and level 4 DiD are different.
  6) DiD level 5 (Node EKP.3.8.5.1) it is not clear how the I&C systems satisfy this aspect (lack of detail).

Annex 3

7) Many sub-claims do not have supporting evidence identified in a suitable manner. Additionally, where a sub-claim references to another SCM the reference is to the entire SCM making tracing the claim, argument, evidence for the EKP3 sub-claim particularly difficult, especially as the referenced SCMs do not have appropriate links in from EKP.3.

The designer or future operator / licensee is requested to produce an update to the SCM covering all aspects of the SAP and addresses the points above.

T13.T02.45 - From the review of the CAE Trail presented in the SCM for EKP.5 the following areas for improvement are raised:

- Sub-claim to para 146(d) 'administrative safety measures' does not provide detail of what I&C systems are claimed and if they are available for all faults (if they are not available what back-up measures are provided). The designer or future operator / licensee is requested to ensure produce an update to the SCM that addresses all applicable C&I systems.

- Sub-claim to para 147 does not adequately address how either availability and reliability of I&C are 'commensurate with the significance of the radiological consequences to be controlled' - for reliability, a reference to the fault schedule could be used here to show that the PMS (1e-3 pfd) and DAS (1e-2 pfd) contribute risk reduction to claimed faults. The designer or future operator / licensee is requested to produce an update to the SCM that identifies the demonstration of how availability and reliability of C&I systems are commensurate with the significance of the radiological consequences they control.

- Some references do not have section numbers. The designer or future operator / licensee is requested to ensure that when evidence is cited the specific sections of the document should be identified.

T13-T02-46 - The designer or future operator / licensee is requested to produce evidence and demonstration of specification and qualification of in-core, ex-core and process sensors. This should include:

- Details of which IEC standards (or equivalent ~ equivalence to be demonstrated) are applied or required of suppliers to apply;

- explanation of how conformance with these standards is demonstrated;

- explanation of how qualification of sensors for both normal and accident environments is addressed.

In addressing the TO, the designer or future operator / licensee may wish to take account of the preliminary response to TQ-AP1000-1174 provided by WEC.

Conclusions of Task Reviews

With regards to SAP conformance demonstration, it is concluded that there are a significant number of areas for improvement in the presented Argument and identified Evidence the CAE Trails in the SCM. The key generic areas for improvement are:

- Inappropriate reference to evidence.

Annex 3

- Lack of clear identification of location of evidence within a document.
- SCM do not address all appropriate systems and platforms.
- Clear 'Argument' not always apparent due to limited information in the 'Sub-claims'.
- Lack of revision control of identified evidence.
- Much of the evidence is not available and is identified in the SCM as 'LATER'.
- No clear identification of specific IEC Standards and Clauses that support the argument and no demonstration of compliance with appropriate international standards or equivalence demonstration.

With regards to the Sensor review, a sample review of the CETs System Design Specifications against IEC 60737:2010 has shown that of 42 clauses reviewed in IEC 60737, there was:

- Compliance with 5 clauses.
- Partial compliance with 12 clauses: Most of these were due to the need for supporting justification and evidence, although some statements only partially covered the issue raised in the standard.
- Non compliance with 25 clauses: Almost all non compliances were because the IIS System Specification did not include content directly addressing the issue identified by the clause in the standard.

With regards to the PCSR and DCD Updates, it is concluded that:

- The up-issue of the PCSR from revision 0 to revision 2 did not included any significant changes in terms of the safety case structure, (including response to the SAPs); the specific claims on the system and supporting argument and evidence trail was still not clear. There was a minor improvement in the report to provide evidence for some specific claims made against a function of a safety-related C & I system.
- The change control notice for the DCD states the document had been revised to include changes to the standard design that were a result of Westinghouse design finalisation reviews and changes committed to US NRC resulting from their review. Although there had been minimal changes, specific modifications relate to determining reactor trip parameters and these will be considered as part of the TSC Task 16 review.

In the opinion of the TSC subject to sufficient and adequate responses being made to the TOs/Potential GDA Issues it is anticipated that an adequate position could be confirmed for:

Demonstration of conformance with HSE / ND C&I SAPS.

Confirmation of design, manufacture, test and qualification of Sensors to international standards.

Annex 4

TSC Task Summary - Review of Systems' Classification and Standards[2]

Note this information has been imported from a TSC report (Ref. 52) and the formatting of the TSC report has been retained.

[2] Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 4

Annex: TSC Task Summary: Review of C&I Classification and Standards – AP1000

This Annex summarises a review of the Control and Instrumentation (C&I) Classification and Standards for the Westinghouse UK AP1000 reactor design. The review was undertaken in Step 4 of GDA by a Technical Support Contractor (TSC) in support of the HSE / ND. The claims and arguments presented by Westinghouse (WEC) were reviewed in the preceding Step 3. The GDA Step 4 review addressed, on a sample basis, the adequacy of the evidence identified in support of the claims and arguments presented in Step 3 relating to C&I Classification and Standards.

The aim of this review has been to gain confidence that Westinghouse as the Requesting Party (RP) has substantiated that:

i. The Categorisation of the C&I safety functions is in accordance with the requirements of the HSE / ND Safety Assessment Principles (SAPs) and International Standards (in particular IEC 61226) and that Classification identified for the major C&I systems performing those functions is also in accordance with the SAPs and International Standards (in particular IEC 61226 and IEC 61513);

ii. The standards and techniques for function categorisation and system classification are appropriate and are consistently applied and that these require the application of appropriate processes and procedures;

iii. The WEC Quality Management System (QMS) prescribes processes that are adequate to ensure compliance with or are equivalent to (at a system level) the principal Nuclear Sector IEC Standards.

This GDA Step 4 review is based on the following aspects with respect to Classification and Standards:

- Open HSE / ND Step 2 and 3 observations;
- Open Step 3 Technical Queries and those raised in this review in Step 4;
- Conformance with HSE / ND SAPs;
- Compliance with agreed International Nuclear Sector Standards.

The planned review of the evidence supplied by WEC was to consider all major clauses of the Level 1 IEC Standards based on the clause by clause analyses supplied by WEC, and to take cognisance of Level 2 IEC Standards and other guidance documents where possible.

The output from the Task 14 review is noted below.

SAPs

A Step 2 observation requested WEC to demonstrate conformance with relevant HSE / ND Safety Assessment Principles, to this end, WEC produced Safety Case Maps (SCM) that were supplied and initially reviewed during Step 3. During GDA Step 4 WEC prepared SCM for all the applicable SAPs and also enhanced the SCM content in the light of feedback. Detailed SAP evidence review tables were produced by TSC based on these SCMs, and the evidence documents identified were reviewed on a sampling basis by all Step 4 tasks. The aim was to determine if the documentation identified in the

Annex 4

SCM contains adequate evidence to support the RP claims and arguments for each applicable SAP in the context of each task. The results for each task review were collated and presented in the Task 11-13 report. The review of SAPs in Task 14 was limited to one; ECS.3 Standards. It was found that conformance with the intent of SAP ECS.3 and supporting paragraphs was not fully demonstrated from the SCM provided and a Technical Observation has been raised accordingly.

Categorisation and Classification

The HSE / ND GDA Step 2 report raised a number of Observations relating to Categorisation and Standards. The HSE / ND GDA Step 3 report raised two more Observations relevant to Categorisation Classification and Standards. Westinghouse advised that because the AP1000 documentation was prepared for the US NRC, the standards used are in accordance with IEEE Std-603-1991, i.e. US Standards have been applied, and acknowledged that for UK licensing, there is a requirement to demonstrate compliance with the Nuclear Sector C&I IEC Standards.

Categorisation

In line with US requirements, C&I functions are identified as either safety related or non-safety rather than the four categories identified in the SAPs and IEC 61226. However, Westinghouse has recognised the UK requirement for the conformance with SAPs and compliance with IEC 61226 by mapping the UK AP1000 functions and systems to the UK requirements in a satisfactory manner.

Classification

During Step 4 the Westinghouse responses to the HSE / ND Step 2 and Step 3 Observations relevant to Classification and Standards were reviewed and Technical Observations were raised where the responses were judged to be insufficient to resolve the Step 2 and Step 3 Observations.

The review noted that the WEC QMS has been developed to comply with US regulator and applicable industry guidelines i.e. to be in accordance with ISO 9001:2000 and ISO 9000-3:1997; and in addition, as applicable for safety-related activities, Appendix B of 10 CFR 50; ASME NQA-1 1994 Edition; and IAEA 50-C-QA Revision 1.

Compliance with International Nuclear Sector Standards

The reviews conducted for alignment of WEC processes to the requirements of relevant IEC Standards is summarised below:

IEC 61513:2001

The IEC 61513 standards compliance evidence provided directly by WEC mostly refers to generic design documents and UK AP1000 / I&C system project documents. Some Company level processes from the QMS Level 2/3 are claimed by WEC, however it is considered that the processes do not adequately demonstrate full accordance with IEC 61513 requirements and thus full accordance cannot be confirmed at this stage.

With respect to Section 5 of IEC 61513, the WEC clause by clause review does not adequately cover consideration of the C&I of the whole plant, identification of functions, their categorisation and

Annex 4

assignment to systems. It does not provide a clear Claims, Arguments, Evidence (CAE) trail to support accordance with Section 5 of IEC 61513 for the UK AP1000.

In summary, the WEC review does not contain sufficient information on Company level processes and the link to system level processes to support a claim that the QMS adequately enables system level processes in accordance with IEC 61513:2001.

IEC 60880:2006

The IEC 60880 standards compliance evidence provided by WEC does not demonstrate full accordance with IEC requirements and thus full accordance cannot be confirmed at this stage.

In summary, the WEC review does not contain sufficient information on Company level processes, and the link to system level processes, to support a claim that the QMS adequately enables system level processes in accordance with IEC 60880:2006.

IEC 62138:2004

The IEC 62138 standards compliance evidence provided by WEC covers most applicable clauses of IEC 62138 and provides a link to the applicable QMS Level 2/3 Policies and Procedures thus most of the identified processes are considered to be broadly in accordance with the requirements. They do not however link to system level processes to support a claim that the QMS adequately enables system level processes in accordance with IEC 62138:2004, e.g. WEC has not provided evidence for IEC 62138 clause 6.2 'Selection of Pre-developed software'.

In summary, the WEC review does not contain sufficient information on Company level processes and the link to system level processes to support a claim that the QMS adequately enables system level processes in accordance with IEC 62138:2004.

IEC 60987:2007

The IEC 60987 standards compliance evidence provided by WEC mostly refers to either UK AP1000 specific documents, WEC generic design documents or UK AP1000 ('WCAP') level documents. Documentation relating to the PMS is referenced against some IEC 60987 clauses. While some clauses have a claim for QMS Level 2/3 processes, it is considered that the processes do not adequately demonstrate accordance with IEC requirements thus full accordance cannot be confirmed at this stage.

It is concluded that a demonstration of accordance of WEC Company level processes to IEC 61513:2001, IEC 60880:2006, IEC 62138:2004 and IEC 60987:2007 may be possible if WEC provide more detailed evidence of Company level processes from the QMS for each IEC clause or provide a justification as to why any non-conformance is acceptable.

The review of evidence as supplied directly by WEC (clause by clause standards compliance matrices) has generated Technical Observations on the adequacy of the RP supplied CAE.

It was intended that Step 4 would provide a sampled review of some Level 2 Standards in addition to the Level 1 Standards. However, the additional effort required to resolve emerging priorities related to other Step 4 tasks has prevented the TSC from undertaking this Level 2 review work.

Annex 4

QMS

During the early Step 4 work it was anticipated that Westinghouse would identify a QMS, supported by a suite of Company-level processes used for all developments, to substantiate a claim of compliance, at a high level, for all C&I systems with the principal Nuclear Sector IEC Standards. However, the early work found difficulties tracing Company-level processes relevant to the principal Nuclear Sector IEC Standards and Technical Queries (TQs) were raised to request identification of the applicable processes from Westinghouse. The responses to the TQs did not provide the required clarity and this topic was pursued at progress meetings. Westinghouse provided a further response in the form of 'QA maps'.

It was recognised via discussions at meetings and the information contained in the QA maps that Westinghouse has an 'enabling QMS', requiring each project to organise its own processes as appropriate and providing requirements for what these processes must include. Despite the fact that TQs requested information on both Company and system level process compliance to Standards, which would have allowed Westinghouse to demonstrate that the system level processes are an implementation of the enabling QMS requirements, the clause by clause Standards review matrices provided by Westinghouse were found to only partly cover Company and system level processes. The TSC review of the compliance of WEC processes with the Nuclear Sector IEC Standards has none-the-less sought to trace such a demonstration for the clauses sampled, using the QA maps and by following a sample of the cited evidence documents.

Whilst there is no UK-specific AP1000 Quality Plan at present, it is understood that this will be prepared by WEC once a UK contract is in place and that this is in accordance with the provisions of the WEC QMS. The requirement for a UK-specific AP1000 Quality Plan is captured by a Technical Observation.

The Westinghouse C&I project plans and programmes have a hierarchical structure and link to relevant WEC QA system procedures although not all relevant QA system procedures are identified in the documents provided. Although the evidence cited by Westinghouse in the clause by clause Standards compliance matrices does provide some level of confidence that appropriate processes have been developed and followed, the evidence presented in the clause by clause exercise is an area for improvement.

A subset of clauses from IEC 61513 was selected for further sampling within this review. For these sampled areas, the TSC reviewed the full route from the Company level processes, through departmental level processes, project level processes (and developmental processes specific to the technology or topic if appropriate) to the system level processes. This was done in order to ascertain the extent to which a claim that the QMS 'enables' lower level processes that are in compliance with the requirements of the Standards can be demonstrated. This review leads to additional Technical Observations regarding the adequacy of the WEC QMS as an enabling QMS for the specific topic areas sampled.

In particular there is a need to demonstrate how the QMS prescribes processes in line with Level 1 Nuclear Sector IEC Standards for the development of C&I systems important to safety and that this applies over the life of the system. Technical Observations have therefore been raised requesting that the links between the QMS processes and the system specific processes they enable are established, and how these ensure compliance with the detailed clauses of the principal Nuclear Sector IEC Standards.

Annex 4

Westinghouse have made claims relating to the compliance of their processes with the Level 2 and 3 IEC Standards, however, evidence is required to substantiate that there are no gaps. This aspect is covered by Technical Observations that request demonstration of compliance and identification of documented evidence to confirm there are no gaps in the compliance of WEC processes to the Level 2 and 3 Standards.

Technical Observations

The HSE / ND GDA Step 2 report raised a number of Observations relating to Classification and Standards. The HSE / ND GDA Step 3 report raised two more Observations relevant to Classification and Standards.

During Step 4 the Westinghouse responses to the HSE / ND Step 2 and Step 3 Observations relevant to Classification and Standards were reviewed and Technical Observations were raised where the responses were judged to be insufficient to resolve the Step 2 and Step 3 Observations.

In addition to the Step 2 and Step 3 HSE / ND Observations, TSC observations have been raised by issuing Technical Queries to Westinghouse during Step 3 and Step 4. As identified below, Technical Queries and Observations that have not been satisfactorily addressed have been merged into a single set of Technical Observations. These TOs capture all the unresolved matters from the review of the evidence supplied by WEC against selected SAPs guidance and Standards. A total of seven Technical Observations have been raised, which have been designated as TO1 or TO2 by the TSC depending on their significance, of which TO1 is the higher significance. One of these observations has been designated as TO1 (with two associated TO2s) and four additional observations have been designated as TO2.

The one TO1 and its two associated TO2 technical observations are:

T14.TO1.01: The designer or future operator / licensee is requested to demonstrate and document that the QMS processes and procedures prescribe processes for the development of C&I Systems Important to Safety (SIS) that are, compliant with / equivalent to, the system level requirements of key (i.e. Level 1) IEC C&I nuclear sector standards and that this is maintained for the life of the SIS. T14.TO2.03 & 04 are linked to this TO1.

> **T14.TO2.03:** The designer or future operator / licensee is requested to identify in the clause-by-clause compliance matrices for the Level 1 IEC C&I nuclear sector standards the QMS procedure for each phase of the lifecycle and essential development activities e.g. configuration management and change control, to demonstrate compliance with or equivalence to the system requirements of the IEC C&I nuclear sector standards.
>
> **T14.TO2.04:** The QMS includes project / platform specific procedures for the design and implementation of C&I SIS. The designer or future operator / licensee is requested to identify and document how the QMS requires that the project / platform specific C&I procedures are included in the C&I quality plan for a specific project, e.g. the UK AP1000, and reference them in the clause-by-clause compliance matrices.

The four other TO2 technical observations are:

Annex 4

T14.T02.01: The designer or future operator / licensee is requested to ensure that once a contract is awarded in the UK, a quality plan for the UK AP1000 C&I is put in place, and to substantiate that the quality plan fulfils the requirements of the relevant International Standards e.g. IEC 61513:2001, IEC 60880:2006, IEC 62138:2004 and IEC 60987:2007.

T14.T02.02: The designer or future operator / licensee is requested to substantiate, e.g. in safety case maps, conformance with all SAPs related to Classification and Standards, particularly ECS.3, and to demonstrate that the intent of the SAPs and their supporting paragraphs is satisfied including the provision of all referenced documents.

T14.T02.05: WEC letter UN REG WEC 000207 responding to GDA action 3 on approach to standards identifies standards and documents claimed equivalent to the Level 2 IEC Standards. The designer or future operator / Licensee is requested to 1) identify and document the evidence to substantiate the equivalence of intent of the identified IEEE standards and other documents with the IEC Level 2 standards and, 2) identify the documented evidence to confirm there are no gaps in the compliance of WEC processes to the similar standards.

T14.T02.06: WEC letter UN REG WEC 000207 responding to GDA action 3 on approach to standards makes claims in respect of level 3 IEC Standards. The designer or future operator / Licensee is requested to identify the evidence to substantiate the claim that there are no gaps in the requirements of the WEC processes and the intent of the level 3 standards.

Conclusion

TSC has reviewed the adequacy of the Westinghouse arrangements for Classification and Standards against the requirements of SAPs and appropriate Nuclear Sector IEC Standards and concludes that the claims, arguments and evidence provided require improvement to support a claim that (i) Standards and techniques appropriate to a system's classification are consistently applied and (ii) the QMS prescribes processes that are adequate to ensure compliance (at a system level) with the principal Nuclear Sector IEC Standards.

In summary, unresolved Observations from Steps 2 and 3 have been merged with those arising from this Step 4 review into an integrated set of Technical Observations with the result that the review has developed seven Technical Observations, one of which is of a higher significance.

The one higher significance Technical Observation relates to a requirement that the future operator / Licensee provides a clause by clause demonstration that the QMS complies with the applicable Level 1 Nuclear Sector C&I IEC Standards for development of 'Systems Important to Safety' for each phase of the lifecycle and essential development activities and that these aspects are included in the C&I quality plan for a specific project, e.g. the UK AP1000.

However, if all of the Technical Observations raised by the TSC are adequately addressed, it is the view of the TSC that there is no reason, on the basis on the information sampled to date, to indicate the WEC QMS is unsuitable to enable the development of system level processes appropriate to the system classifications and in accordance with the applicable IEC Standards.

Annex 5

TSC Task Summary - Review of System Platforms and Pre-Developed Components [3]

Note this information has been imported from a TSC report (Ref. 58) and the formatting of the TSC report has been retained.

This Annex refers to the Pre-Construction Safety Report (PCSR) and European Design Control Document (DCD), which are references to the:

> AP1000 Pre-construction Safety Report, UKP-GW-GL-732 Revision 2, Westinghouse Electric Company LLC, December 2009, (Ref. 22); and
>
> AP1000 European Design Control Document, EPS-GW-GL-700 Revision 1, Westinghouse Electric Company LLC, December 2009, (Ref. 27);

respectively.

The versions of the BSCs referred to in this Annex are:

> PMS UKP-PMS-GLR-001 Rev 0 November 2010 (Ref. 49).
>
> CIM UKP-PMS-GLR-002 Rev 0 November 2010 (Ref 98).
>
> DAS UKP-DAS-GLR-001 Rev 0 November 2010 (Ref. 50).

[3] Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 5

ANNEX: TSC Task Summary: Review of System Platforms and Pre-Developed Components

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of the platforms and pre-developed equipment for the Westinghouse UK AP1000 reactor design.

This review follows on from the review of the safety claims and supporting arguments for platforms and pre-developed equipment as a preliminary activity during Step 3. The aim of this review has been to gain confidence that Westinghouse has adequate evidence to support the claims and argumentation presented for the conformance of the platforms and pre-developed equipment to appropriate guidance and standards, including Safety Assessment Principles (SAPs), Technical Assessment Guides (TAGs) and international Nuclear Sector Standards.

The C&I platforms considered form the building blocks of the systems identified in Chapter 6.7 of the UK AP1000 Pre-Construction Safety Report (PCSR) and Chapter 7 of the Design Control Document (DCD). The system platforms and pre-developed components chosen for review comprised the following Class 1, 2 and 3 equipment:

- Protection and Safety Monitoring System (PMS) using Common Q including:
    - the AC160 Common Q platform,
    - the CIM (Component Interface Module) priority logic,
- Diverse Actuation System (DAS) using the Westinghouse 7300 series equipment including the manual interface equipment,
- Distributed Control and Information System (DCIS) using the Ovation platform developed by Emerson including:
    - the Control System (PLS),
    - the Data Display and Controls System (DDS),
- SMART sensors used within the UK AP1000 reactor design,
- OCS (Operation and Control Centre System) Class 1 Displays and Controls,

The PMS, the primary protection system for the UK AP1000, is distributed across four divisions and is based on ABB AC160 technology. The AC160 is a microprocessor based system, which executes software. AC160 software baseline 1.2/0 was used as the input to Westinghouse's Product Software Qualification (PSQ) project. Baseline 1.3/0 includes the modifications identified in the PSQ project and became known as the 'nuclear version'. There have since been other modifications resulting in baseline 1.3/8. This is the version identified for the Generic Design Assessment (GDA) Step 4. The CIM is considered part of the PMS, the PLS controls various safety components via the CIM under supervision of the PMS via priority logic implemented in the CIM. The CIM is produced by CS Innovations (CS-I) a wholly owned subsidiary of Westinghouse.

The DAS is a safety system that provides; an alternative (to PMS) means of initiating reactor trip, actuation of selected Engineered Safety Features (ESF) and monitoring plant information.

Annex 5

The PLS consists of closed loop controllers and the DDS/OCS interface provides the functions required for normal operation from cold shutdown through full power.

Other C&I subsystems such as those listed below, are outside the scope of this review. However any observations made whilst reviewing the systems listed above, which pertain to these out of scope systems, have been recorded and tracked by Technical Observations (TOs).

- In-core Instrumentation System (IIS),
- Turbine Control System (TOS),
- Special Monitoring System (SMS), and
- Radiation Monitoring System (RMS),

For the platforms and pre-developed equipment the intention was to review a sample of the Westinghouse identified evidence for the individual platforms and pre-developed equipment against a selection of the requirements of relevant guidance and standards, identified by HSE / ND,

The eleven key SAPs considered were:

- EQU.1 - Qualification procedures, EDR.1 - Failure to safety, EDR.2 - Redundancy, diversity and segregation, EDR.3 - Common cause failure, ESS.1 - Requirement for safety systems, ESS.21 - Reliability, ESS.23 - Allowance for unavailability of equipment , ESS.27 - Computer based safety systems, ESR.3 - Provision of controls, ESR.5 - Standards for computer based equipment, ESS.15 - Alteration of configuration, operational logic or associated data.

Four Level 1 IEC Standards were considered:

- IEC 61513, IEC 60880, IEC 62138 and IEC 60987,

Three TAGs were considered:

- TAG 003, TAG 046 and TAG 051.

The intention was to report on the following aspects of the individual C&I platforms relevant to this review:

- Review the Technical Queries (TQs) raised in Step 3 Task 5 that were not closed in Step 3, and responses to TQs raised in Step 4,
- Review samples of the evidence identified by Westinghouse in support of claims that relevant SAPs have been satisfied,
- Review samples of the evidence identified by Westinghouse to demonstrate that relevant IEC Standards clauses as agreed with the HSE / ND have been complied with,
- Review Westinghouse responses to Observations raised by HSE / ND during Step 2 and Step 3 that relate to safety and safety-related systems.

It was established that the Westinghouse UK AP1000 PCSR and supporting documentation did not provide a clear Claims, Arguments and Evidence (CAE) trail and Safety Case for the safety and safety-related C&I equipment. While the Safety Case Maps (SCM), introduced to identify the evidence of SAP conformance, gave additional information, they were not sufficiently detailed in terms of arguments and referenced evidence to demonstrate the suitability of the platforms and the adequacy of the

Annex 5

related safety arguments. These observations were discussed with Westinghouse in a series of meetings including:

- meetings to facilitate understanding of, the Oskarshamn document set, and the documents supporting the CIM, and for HSE / ND and TSC to have access to proprietary supplier information, and
- meetings to aid understanding of the revised DAS platform

These, in turn, resulted in Westinghouse supplying additional documentation on the technologies.

In addition HSE / ND requested, via Regulatory Observations 78, 100 & 101 and a Technical Query, that Westinghouse produce Basis of Safety Case (BSC) documents for the platforms and associated systems. The Westinghouse responses to these requests were reviewed by the TSC, leaving the Class 2 / 3 Ovation platform to last.

The following activities were undertaken:

- three separate reviews of the Westinghouse / ABB processes and proprietary documentation were conducted at ABB Stonehouse, Gloucester, for pre-developed AC160 components,
- two separate reviews of the CS-I processes and proprietary documentation proposed for the UK AP1000 CIM were conducted jointly with Westinghouse, and
- the BSC documents for the platforms were reviewed.

As a result of the activities listed above, the intended Step 4 review of platforms and pre-developed equipment was modified to address the following specific areas:

- review of responses to HSE / ND Step 2 Observations identified in the HSE / ND Step 2 C&I Assessment report, as applicable to platforms and pre-developed equipment,
- review of responses to the technical observations from the TSC Step 3 report on platforms and pre-developed equipment
- review of responses to HSE/ND Step 3 Observations identified in the HSE / ND Step 3 C&I Assessment report, as applicable to platforms and pre-developed equipment,
- review of Westinghouse responses to Step 3 and Step 4 TQs as applicable to platforms and pre-developed equipment, and
- review a sample of the CAE in the SCM and BSC submissions (PMS, CIM and DAS) to consider if an adequate demonstration of conformance with HSE / ND SAPs; EQU.1, EDR.2, ESR.5, ESS.21 and ESS.27, has been presented,

Additional activities conducted were:

- technical meetings with Westinghouse and the HSE / ND to provide clarification of TQ subject matter,
- review of evidence documents on the AC160 and the CIM made available by Westinghouse under their supervision; AC160, 3 meetings and CIM, 2 meetings,
- review of the adequacy of the Safety Case presented in the BSC documents for the PMS, CIM and DAS, and
- the creation and iterative review with Westinghouse of a Deviation Matrix addressing hardware and software observations associated with the pre-developed AC160 components,

Annex 5

The findings from the review have been presented as a series of observations that summarise all elements of the review activities identified above. These are identified below as TSC technical observations. A total of 68 technical observations have been raised, these observations have been labelled as TO1 or TO2 by the TSC depending on their significance, of which TO1 is the higher. 14 of the observations have been designated as TO1 and 54 observations have been designated as TO2. Where it is judged that a sufficient number of TO2s have been identified on a topic, a single TO1 is used to provide focus on the topic.

AC160 Platform

Whilst the AC160 has been shown to meet some of the Class 1 requirements placed on it, there is scope for improvement in the following areas:

- QMS, processes, procedures and planning supporting the AC160,
- completeness and application of Verification and Validation,
- the adequacy of the PMS BSC, traceability of the documentation set and resolution of open Deviation Matrix items, and
- the provision of a suitability evaluation, descriptions of communications protocols and completeness of the Westinghouse's documentation set.

During the review to establish the safety capability of the AC160, observations have been made which are detailed in the 4 TO1s and 21 TO2s below:

QMS

T15.TO1.02: The designer or future operator / licensee is requested to review the AC160 procedures for:

- the QMS, processes, procedures and planning supporting the AC160,
- programmable complex electronic components,
- standards compliance, and
- change management and software build

and ensure the points raised in the TO2s below are addressed:

> T15.TO2.01: The review of AC160 software and complex hardware identified areas for improvement relating to traceability of claims, arguments and evidence for Production Excellence, Compensating Measures and Independent Confidence Building Measures. The designer or future operator / licensee is requested to produce updated and consistent versions of the Basis of Safety Case, Final Quality Assessment and Justification Report and Product Specification to ensure the documents address the following:
>
> a. record the Production Excellence argument and identify Compensating Measures in the case where Production Excellence is not achieved, e.g. 'PC Elements' partition,

Annex 5

b. record adequate configuration information, that identifies the configuration version of all items referenced in the three documents,

c. respond to all points raised during the Stonehouse reviews ([1] and [2]),

d. document the claims for Production Excellence for Programmable Complex Electronic Components (PCEC) along with Compensating Measures; these along with confidence building activities, and other means should be documented in the BSC to demonstrate the adequacy of the PCECs for use in a Class 1 safety system, and

e. as the AC160 software is divided into functional partitions, as a minimum the claims, arguments and evidence should be documented at this level by the inclusion of a Partition Claims and Documentation Matrix in the Basis of Safety Case document.

T15.T02.05: The review of the AC160 software and hardware identified areas for improvement relating to the Configuration and Change Management particularly those for changes made after the nuclear baseline 1.3/0 was established following completion of the Final Quality Assessment and Justification Report (FQAJ) exercise. The designer or future operator / licensee is requested to update all relevant documentation, recording the following:

a. the configuration versions should be identified for each release of AC160 since 1.3/0 baseline. This should include all deliverable source and target software, non-deliverable source and target software, project and build files, life-cycle documentation and products should be identified and demonstrated to be complete,

b. the software module versions that constitute the software build proposed for GDA Step 4 (1.3/8) AC160 platform should be defined,

c. the configuration and change management processes pertaining for each change to the software should be identified, and

d. the hardware changes between subsequent versions of the processor module should be identified and it stated how these relate to versions which have been qualified

T15.T02.09: The review of the AC160 software and hardware identified areas for improvement relating to the adequacy of the records of employee capability, methods of assessment, definition of responsibilities and therefore clarity of the suitability for their particular role within the lifecycle of the AC160 product. The designer or future operator / licensee is requested to identify the processes and procedures which pertain and through the evidence of QA audit reports, demonstrate that these processes and procedures have been followed.

Annex 5

T15.TO2.27: The review of the AC160 software and hardware identified areas for improvement relating to the adequacy of the development of PCEC within the AC160. The designer or future operator / licensee is requested to:

a. produce a clearly documented configuration index of the PCEC lifecycle products to fully define the PCECs to be used in AC160,

b. demonstrate that the requirements are traceable from inception, through implementation to test,

c. demonstrate that the planning documents are consistent with the processes and that the implementation of the plan is consistent with the plan,

d. produce a justification to show that the PCEC in the Quint power supply will not impact the safety operation of the power supply.

T15.TO2.28: The review of the AC160 software and hardware identified areas for improvement relating to the adequacy of the documentation of build instructions for the AC160 platform software. The designer or future operator / licensee is requested to document:

a. an integration tree for all of the software modules in the current release of the AC160 platform,

b. the compiler/linker switches used to build the platform software for the current version to ensure that the reason for their use on each occasion when the compiler/linker is invoked is clearly justified, and

c. the configuration/change management process used to build the platform software using 'makefiles' .

T15.TO2.06: The review of the AC160 software and hardware identified areas for improvement relating to the adequacy of the QMS following the nuclear baseline 1.3/0 was established following completion of the FQAJ exercise. The designer or future operator / licensee is requested to:

a. identify the particular processes, procedures and plans (and their versions) which pertained, for each change, during the maintenance phase of pre-developed hardware and software should be clearly identified, this should include any new requirements introduced during this phase, and

b. justify the processes and procedures used for change requirements capture and management, including those which pertain to requirements management tools.

T15.TO2.34: The review of the AC160 software and hardware identified areas for improvement relating to the adequacy of the evidence of adherence to applicable processes since 1.2/0 AC160 software baseline. The designer or future operator / licensee is requested to identify and demonstrate adherence to:

Annex 5

a. the process(es) used to establish the reliability of all hardware modules used in UK AP1000 PMS,

b. the process used to control problem reporting, and

c. the platform Verification and Validation (V&V) plan.

T15.TO2.46: The review of the AC160 software and hardware identified areas for improvement relating to the adequacy of the demonstration of compliance to applicable IEC Standards. The designer or future operator / licensee is requested to produce:

a. a demonstration of compliance of processes and procedures to applicable IEC Standards, during the development life-cycle of the AC160 platform software and hardware, for which Production Excellence is being claimed, and

b. clearly documented Compensating Measures where compliance to applicable development standards cannot be demonstrated.

Verification and Validation

T15.TO1.03: The designer or future operator / licensee is requested to review the:

- completeness and application of V&V to the AC160 platform software,
- use of operational experience,
- source code analysis,
- testing,
- environmental qualification, and
- Independent Confidence Building Measures

and ensure the points raised in the TO2s below are addressed:

T15.TO2.03: The review of the AC160 software and hardware identified areas for improvement relating to the operational experience claims and applicability to versions of the AC160 platform software. The designer or future operator / licensee is requested to produce a substantiation to demonstrate the adequacy of the data collection methods and of the data collected.

T15.TO2.04: The review of the AC160 software and hardware identified areas for improvement relating to the AC160 platform equipment EMC and environmental qualification. The designer or future operator / licensee is requested to document the justification of:

a. the use of a representative AC160 system for environmental qualification, rather than the complete UK AP1000 PMS, and

Annex 5

b. the use of a representative AC160 system for EMC testing, rather than the complete UK AP1000 PMS

T15.TO2.07: The review of the AC160 software and hardware identified areas for improvement relating to deficiencies in the AC160 platform source code analysis. The designer or future operator / licensee is requested to:

a. produce a justification, that the system is deterministic, based on a random distribution of system ticks (interrupts created by the periodic interval timer) relative to the microprocessor cycles, and

b. identify and document confirmation of all source code modules that have been analysed and documented including those which are new since version 1.3/0,

T15.TO2.08: The review of the AC160 software and hardware identified areas for improvement relating to use of new and previously developed test specifications and their use for regression testing of the AC160 platform. The designer or future operator / licensee is requested to:

a. clearly identify and document the scope of the TUV third party tests and the ABB tests and document the justification of the adequacy of these with regards to the Requirements Specification,

b. document the test coverage statistics, in particular where regression testing has taken place; this should include white and black box testing,

c. justify and document the basis for generating test specifications from the commercial version or from the code and/or high level user descriptions and the coverage of these tests,

d. demonstrate and document confirmation that regression testing has been carried out following a change, and

e. document that all relevant test records are under configuration control and that they are complete and relevant.

T15.TO2.30: The review of the AC160 software and hardware identified areas for improvement relating to qualification of tools used in the AC160 platform. The designer or future operator / licensee is requested to produce a document to identify evidence that the development life-cycle of the new 'backtranslate' tool has been assessed as suitable for use in the development of application code for UK AP1000 PMS.

T15.TO2.32: The review of the AC160 software and hardware identified areas for improvement relating to software hazard analysis, software reliability and safety level partitioning in the AC160 platform. The designer or future operator / licensee is requested to produce a substantiation[4], to:

[4] ND Clarification: the substantiation should be included in or referenced from the BSC.

Annex 5

a. clarify the process used for a software hazard analysis in the platform and demonstrate that it has been applied,

b. justify the use of the VRTX operating system in the AC160 platform,

c. justify the claim that changes to the software since 1.3/0 are only bug fixes, this may impact the Safety Criticality Assessment, and

d. explain the change to the Software Criticality Index of the 'backtranslate' tool.

T15.TO2.39: The review of the AC160 software and hardware identified areas for improvement relating to requirements traceability since the 1.2/0 AC160 software baseline. The designer or future operator / licensee is requested to document:

a. the full traceability of requirements through to test for the PCECs,

b. the justification of the basis for generating test specifications from the non-nuclear version and the coverage of these tests,

c. the justification of the basis for generating test specifications from the code and/or high level user descriptions and the coverage of these tests, and

d. a review of the change requirements traceability for the 1.2/0 AC160 software baseline onwards for the AC160 platform, to confirm that requirements can be traced from inception, through implementation to test.

T15.TO2.40: Commitment has been made to carry out statistical testing and a MALPAS analysis. The designer or future operator / licensee is requested to produce a detailed explanation of the proposed methods and how these will be used primarily for Independent Confidence Building Measures and also whether any claims will be made for their use as Compensating Measures. A justification of the suitability of the approach should also be produced.

BSC and Other Observations

During the review of the AC160 observations were also made on the following topics:

- adequacy of the BSC,
- traceability and consistency of the AC160 documentation,
- resolution of open Deviation Matrix items at the end of Step 4,
- the provision of a suitability evaluation,
- descriptions of communications protocols, and
- completeness of the Westinghouse documentation.

The following TO1s and TO2s should be addressed in this context:

Annex 5

T15.TO1.11: The designer or future operator / licensee is requested to review the:

- adequacy of the BSC,
- traceability and consistency of the AC160 documentation, and
- resolution of open Deviation Matrix items at the end of Step 4,

and ensure the points raised in the TO2s below are addressed:

T15.TO2.63 (T16.TO1.01): The review of the AC160 software and hardware identified areas for improvement relating to adequacy of the PMS Basis of Safety Case. The designer or future operator / licensee is requested to produce a revised BSC to incorporate:

a. a substantiation of the surveillance of the integrity of content of the flash memory, Mirror RAM, Global Memory devices as part of the diagnostics in ESS.21,

b. an explanation of the distributed interpreter or point to the document which does explain it,

c. a Partition Claims and Documentation matrix to consolidate the Production Excellence, Independent Confidence Building Measures and Compensating Measures claims with the supporting documentary evidence, and

d. all review comments on the BSC formally transmitted to Westinghouse.

T15.TO2.35: The review of the AC160 software and hardware identified areas for improvement relating to traceability and consistency of all applicable documentation in the AC160 platform. The designer or future operator / licensee is requested to produce updates to the Basis of Safety Case, Final Quality Assessment and Justification Report, Product Specification and any other applicable documentation, addressing the following:

a. ensure that the Basis of Safety Case, Final Quality Assessment and Justification Report and Product Specification to documents together:

   i. include the Production Excellence argument and identify Compensatory Measures in the case where Production Excellence is not achieved,

   ii. the three documents are consistent,

   iii. include adequate configuration information, that identifies the configuration version of all items referenced in the three documents, and

Annex 5

iv. address all points raised during the Stonehouse reviews ([1] and [2]),

b. produce a full AC160 platform document map for each release of software and firmware.

T15.TO2.65: The review of AC160 software and hardware identified areas for improvement. These observations were collated and tracked in the Deviation Matrix. The designer or future operator / licensee is requested to document the resolution of the open items in the Deviation Matrix, developed during the review of the AC160 platform, and to include the completed matrix in the PMS BSC.

T15.TO2.37: The review of the AC160 identified that a suitability evaluation is not available for the use of the AC160 platform in the UK AP1000 PMS. The designer or future operator / licensee is requested to produce a suitability evaluation for the use of the AC160 platform in the UK AP1000 PMS.

T15.TO2.43: The review of the AC160 software and hardware identified areas for improvement relating to adequacy of the description of communications protocols used within the AC160 platform. The designer or future operator / licensee is requested to document[5]:

a. the detail of how postulated failures are handled by the HSL protocol, and

b. all communications paths used in the AC160 platform, in detail.

T15.TO1.12: In addition to addressing the main observations recorded above the designer or future operator / licensee is requested to address the individual observations in Section 3.6.1 of TSC Report (FNC37194-37352R)[6], and update the PMS BSC and Westinghouse development procedures as appropriate.

Component Interface Module

Whilst the CIM has been shown to meet some of the Class 1 requirements placed on it, there is scope for improvement in the following areas:

- QMS, processes, procedures and planning supporting the CIM,
- completeness and application of Verification and Validation and requirements traceability, and
- the adequacy of the PMS BSC, substantiation of reliability targets, statistical testing and adequacy of overall CIM documentation.

[5] ND Clarification: the substantiation should be included in or referenced from the BSC.

[6] ND Note: see Ref. 58 in Section 6 of the main body of this report.

Annex 5

During the review to establish the safety capability of the CIM, observations have been made which are detailed in the 6 TO1s and 10 TO2s below:

QMS

T15.TO1.07: The designer or future operator / licensee is requested to review the CIM procedures for:

- the QMS, processes, procedures and planning supporting the CIM,
- responsibilities of those involved in assessment and review activities,
- CAE for Production Excellence, Compensating Measures and Independent Confidence Building Measures,
- configuration and change management,
- adherence to IEC Standard compliant processes, and
- programmable complex electronic components,

and ensure the points raised in the TO2s below are addressed:

T15.TO2.10: The review of CIM hardware identified areas for improvement relating to the claims, arguments and evidence supporting the adequacy of the QMS and its processes. The designer or future operator / licensee is requested to produce a substantiation to:

a. show compliance of Westinghouse and CS-I processes, including V&V documents, to appropriate IEC Standards and SAPs, e.g. through the use of the PCEC checklist.

b. demonstrate a precise CS-I product life-cycle that shows clearly how CS-I decomposes Westinghouse requirements and reviews and validates the decomposition, and

c. demonstrate the existence and application of a CS-I gated process for the CIM development and maintenance.

T15.TO2.11: The review of CIM hardware identified areas for improvement relating to the explanation of responsibilities for those involved in assessment and review activities and hence the claims, arguments and evidence to demonstrate independence. The designer or future operator / licensee is requested to document:

a. how the CS-I design process supports the CIM design life-cycle, showing when board reviews and tests are conducted and describing how independence is achieved between design, board review and test activities (e.g. do different people undertake each?), and

b. how and when independent third party assessment of the CIM will be achieved and showing that this strategy is appropriate for the safety/reliability claim on the CIM.

Annex 5

T15.TO2.15: The review of CIM complex hardware identified areas for improvement relating to traceability of claims, arguments and evidence for Production Excellence (PE), Compensating Measures (CM) and Independent Confidence Building Measures (ICBM) for each hardware and software component. The designer or future operator / licensee is requested to produce an updated Basis of Safety Case, to include:

a. a description of how the PMS safety requirements are fed down to the CIM development process and how PMS related safety hazards, found during the CIM safety hazard analysis process, are fed back to the PMS development process, this should include a description of how the results of the FMEA drive the requirements and design, and

b. a thorough discussion and justification for PE, CM and ICB in the context of the target reliability for the CIM.

T15.TO2.16: The review of CIM hardware identified areas for improvement relating to the CIM Configuration and Change Management of processes and products. The designer or future operator / licensee is requested to:

a. include in the BSC a clear chronology for, and description of, the evolution of the CIM (including different releases of the CIM); this should cover, for example, the CIM redesign project, which is only mentioned in passing in current documentation,

b. produce a documented configuration index which should include: Hardware components; PCEC firmware components; and supporting documentation, and

c. document a review to substantiate the CIM claims, arguments and evidence and related documentation, to confirm that the CIM Configuration and Change Management processes and products are comprehensively and clearly documented.

T15.TO2.42: The review of CIM hardware identified the need for additional evidence that a defined process has been followed. The designer or future operator / licensee is requested to document:

a. a description showing how, in the context of IEC 61513, the system safety requirements have been considered throughout the design life cycle of the PCEC, e.g. firmware safety hazard analysis at all levels of the PCEC life cycle, the scope of the description should include as a minimum processes for design, procurement, V&V and Independent Verification and Validation (IV&V). Evidence should be providing that shows these processes have been followed,

b. how the non functional requirements are passed between Westinghouse and CS-I e.g. those that are passed through via the procurement specifications; and

c. in the CIM BSC, a description of the system V&V identifying the outputs from the design review and providing examples as evidence.

Verification and Validation

Annex 5

T15.TO1.08: The designer or future operator / licensee is requested to review the CIM procedures for:

- clarity of V&V and IV&V activities, and
- requirements traceability

and ensure the points raised in the TO2s below are addressed:

> T15.TO2.12: The review of CIM hardware identified areas for improvement relating to the clarity of V&V and IV&V activities. The designer or future operator / licensee is requested to document:
>
> a. the explanation and evidence to justify that the CIM SRNC V&V Plan is in accordance with SAPs and IEC Standards,
>
> b. a description of the design lifecycle products (e.g. review reports) in relation to the FPGA V&V and IV&V (the CIM BSC only describes implementation products e.g. design and V&V specifications and results), and
>
> c. a clear description of all phases of the CIM V&V process; as the two CS-I phases of V&V, the Westinghouse IV&V, the Westinghouse fourth phase of V&V and the final phase of V&V is confused and unclear, the description should include, for the phases, their time line, inputs, outputs and purpose.
>
> T15.TO2.13: The review of CIM hardware identified areas for improvement relating to CIM requirements traceability. The designer or future operator / licensee is requested to document how the PMS requirements have driven the design and been followed through the design of the CIM.

BSC and Other Observations

During the review of the CIM the following topics were identified:

- adequacy of the BSC,
- substantiation of reliability targets,
- justification of the complexity of the CIM,
- descriptions of communications protocols,
- statistical testing, and
- adequacy of the overall CIM documentation set

The following TO1s and TO2s should be addressed in this context:

> T15.TO1.05: The review of CIM hardware identified areas for improvement relating to the adequacy of the CIM BSC document. The designer or future operator / licensee is requested to produce a revised BSC to incorporate:

Annex 5

a. references to a significantly increased and more comprehensive evidence trail as the document reviewed contains many claims and some arguments but little evidence,

b. an overview of, and references to, tools and their qualification, and

c. clarification and identification of references to evidence that supports what happens when a CIM error is detected, i.e. do outputs go to a defined state?

T15.TO1.06: The review of CIM hardware identified areas for improvement relating to the clarity of the CIM reliability target and substantiating evidence of compliance of the actual CIM reliability with this target. The designer or future operator / licensee is requested to document (possibly in the CIM BSC):

a. a justification of how the use of a dual core in the CIM Field Programmable Gate Array (FPGA) contributes to reliability, as opposed to just adding complexity, and why duplicating just the 'core logic' in the FPGA is sufficient (e.g. without also duplicating other functions or having diversity in the hardware descriptive language used to program the FPGA), and

b. a description of the scope and frequency of testing and how revealed-unrevealed / safe-dangerous failures from the FMEA have been taken into account in determining the testing required. This should include stating the proof test interval and how it has been derived from, or contributes to achievement of, the reliability targets.

T15.TO2.61: The review of CIM hardware identified areas for improvement relating to the adequacy of the argument justifying the complexity of the CIM. The designer or future operator / licensee is requested to produce an update to the Basis of Safety Case for the CIM which addresses the claims, arguments and evidence supporting:

a. SAP ERL.1 (form of reliability claim), taking into account the implications of the novel and complex nature of the design, for arguments supporting reliability claims. For example, for such designs there may not be relevant historical reliability data available. Thus reliability arguments need to be developed from consideration of factors, e.g. the scientific and technical issues involved, precedents, additional independent assessment and best practice, and

b. SAP ERL.2 (measures to achieve reliability), including consideration of systematic failures for this complex, software based design process.

T15.TO2.62: The review of CIM hardware identified areas with potential for improvement in the adequacy of the description of communication protocols and adequate partitioning of communication paths. The designer or future operator / licensee is requested to document:

a. the X bus failure detection, describe the step by step failure detection process (ideally including a flowchart) for the CIM communication errors associated with the 'X bus' and High Speed Link (HSL); the description should include how PMS demands are addressed when an X bus link has failed and how any failure

Annex 5

requirements stated in CIM related requirements and design specifications are addressed,

b. how suitable partitioning of the communications paths in the CIM is achieved, ensuring that one communication path cannot corrupt others such that safety is not compromised, in particular the PLS communications should not be allowed to corrupt the PMS communication path or PMS actions, and

c. a description of the communications protocol for all communication paths in and out of the CIM.

T15.TO2.66: Commitment has been made to carry out statistical testing on the PMS. The designer or future operator / licensee is requested to explain the contribution of the PMS statistical testing to the CIM safety justification.

T15.TO1.10: The review of CIM hardware identified areas for improvement relating to the adequacy of the overall CIM documentation set. The designer or future operator / licensee is requested to produce an update to CIM documentation set for the UK AP1000 to include:

a. a justification that the processes for the purchase and dedication of the CIM FPGA are appropriate for equipment intended for use in a Class 1 System,

b. identification of roles, responsibilities, authorities and accountabilities,

c. a clarification of the CIM project internal audit activities, processes and records,

d. a clarification of the process used for hardware verification and validation and justify its adequacy,

e. a justification of the adequacy of the configuration control of tools,

f. a demonstration of the adequacy of the Automatic Test Equipment tool including its development lifecycle and its qualification for use with Class 1 equipment, and

g. identification of the full range of 'freeze' points (e.g. for V&V) required to allow the processes to be successful. This should include references to any substantiating documentation.

T15.TO1.13: In addition to addressing the main observations recorded above the designer or future operator / licensee is requested to address the individual observations in Section 3.6.2 of TSC Report (FNC37194-37352R), and update the CIM BSC and Westinghouse / CS-I development procedures as appropriate.

7300 Series Equipment

Whilst the 7300 Series Equipment has been shown to meet some of the Class 2 requirements placed on it, there is scope for improvement in the following areas:

- QMS, processes, procedures and planning supporting the 7300 Series equipment,

Annex 5

- completeness and application of Verification and Validation, and
- the adequacy of the DAS BSC.

During the review to establish the safety capability of the 7300 Series Equipment, observations have been made which are detailed in the 1 TO1 and 13 TO2s below:

QMS

The following topics were identified in respect of the QMS, processes, procedures and planning supporting the 7300 Series equipment:

- the applicability of US standards and practices,
- personnel competency management,
- claims, arguments and evidence supporting the development of each hardware component,
- configuration / change management,
- justification of the Class 2 system performing a Category A function,
- Identification of activities in the Safety Plan,
- legacy procedural inconsistencies, and
- compliance with SAPs and IEC Standards.

The following TO2s are relevant in the context of the above:

T15.TO2.14: The review of the 7300 series equipment identified that it was developed to US standards and practices. Observations have been made in respect of compliance with IEC Standards in the UK. The designer or future operator / licensee is requested to document:

a. argumentation showing that the development process meets the intent of the relevant IEC Standards, and

b. a clause by clause compliance analysis for the DAS for IEC 61513.

T15.TO2.67: During the review of the 7300 series platform, observations have been made in respect to personnel competency management. The designer or future operator / licensee is requested to document how personnel are demonstrated to be competent to undertake the tasks to which they are allocated and how records to this effect are maintained.

T15.TO2.16: The review of 7300 series equipment identified areas for improvement relating to the claims, arguments and evidence supporting adequacy of development for each hardware component. The designer or future operator / licensee is requested to document:

a. the design substantiation for the 7300 series pre-developed boards specified for use in UK AP1000 DAS application, and

Annex 5

b. the evidence supporting the proven in use argument, that should identify the 7300 board part numbers and exact revision for the selected UK AP1000 DAS equipment together with specific data of operational hours and the defect history records.

T15.TO2.18: The review of 7300 series equipment identified areas for improvement relating to configuration / change management processes and products. The DAS BSC states the platform design is very mature with over 35 years of production and design improvements. The designer or future operator / licensee is requested to:

a. reference, in the BSC, the process used to make the design improvements, and

b. produce a justification that the change management process is adequate to meet the requirements of IEC Standards, e.g. IEC 61513.

T15.TO2.19: The review of 7300 series equipment identified areas for improvement relating to the claim that it is acceptable for a Class 2 system performing a Category A function. The designer or future operator / licensee is requested to produce argumentation and evidence, in the BSC, for relaxing the Classification of the DAS from a Class 1 to Class 2 safety system.

T15.TO2.20: The review of 7300 series equipment identified areas for improvement relating to the identification of activities which are required to be specified in the BSC. The designer or future operator / licensee is requested to include the following in the BSC:

a. through life test and surveillance and record keeping, and

b. evidence to support the SAP ECM.1 claims.

T15.TO2.53: The DAS BSC states that 'legacy procedural inconsistencies' between the original 7300 development process and the current QMS have been resolved. It is requested that the designer or future operator / licensee should reference in the DAS BSC the document which identifies all of the 'legacy procedural inconsistencies' and how they were resolved.

Verification and Validation

During the review of the 7300 Series equipment the following topics were identified in respect of the completeness and application of V&V:

- substantiation of Operational Experience,
- V&V processes and Environmental Qualification,
- applicability of FMEA to claims on proposed equipment,
- reliability and failure modes, and

The following TO2's should be addressed in this context:

T15.TO2.21: The review of 7300 series equipment identified areas for improvement relating to Operational Experience claims and applicability to particular revisions of the platform

Annex 5

hardware. The designer or future operator / licensee is requested to substantiate the operational experience claims and the applicability to particular revisions of the platform hardware. In addition, the designer or future operator / licensee is requested to produce a justification for the reliability analysis, that includes proven in use data to substantiate the Mean Time Before Failure (MTBF) figures and hence the reliability claim made on the DAS.

T15.T02.22: The review of 7300 series equipment identified areas for improvement relating to production V&V process and environmental qualification of the final product and their applicability to particular versions of the platform hardware. The designer or future operator / licensee is requested to:

a. produce a demonstration that V&V is performed for the 7300 platform equipment, as part of the production process,

b. produce a demonstration that the latest 7300 modules proposed for the UK AP1000 DAS application have undergone equipment qualification testing, or produce evidence of any module modifications and the substantiation for not re-qualifying the equipment, and

c. demonstrate that the 7300 equipment meets the environmental requirements of IEC 60780, IEC 60980 and IEC 61000 series standards.

T15.T02.24: The review of 7300 series equipment identified areas for improvement relating to the applicability of any existing FMEA to claims on the proposed equipment. The designer or future operator / licensee is requested to document confirmation that:

a. there will be a documented FMEA that determines revealed / unrevealed and safe / dangerous failures for the 7300 series equipment selected to be used in the UK AP1000 DAS application,

b. the document WCAP-14036-P-A 'elimination of periodic protection channel response time tests' defines the scope of the FMEA to be performed, and

c. that the six monthly testing of the DAS is consistent with the proof test frequency necessary to meet the reliability targets for the DAS.

T15.T02.25: The review of 7300 series equipment identified areas for improvement relating to the established 7300 reliability and failure modes. The DAS BSC states a comprehensive reliability programme has been performed to ensure the DAS is reliable and inherently safe. The designer or future operator / licensee is requested to document a clarification of whether the 7300 series modules have been designed and configured such that they have a 'safe' or 'preferred' failure mode and similarly with the architecture of the DAS itself.

T15.T02.26: The review of 7300 series equipment identified areas for improvement relating to the clarity of the reliability calculations. The designer or future operator / licensee is requested to document:

a. the failure rates for each board contributing to the overall failure rates presented in DAS BSC, and

Annex 5

b. a discussion of the reliability based SAPs that should include the quantitative conclusions of the Probabilistic Risk Assessment to justify the reliability claims made in the SAP compliance section of the DAS BSC.

BSC

T15.TO2.64 (T16.TO1.03): The review of 7300 series equipment identified areas for improvement relating to the potential for improvement in the adequacy of the DAS BSC document. The designer or future operator / licensee is requested to produce a revised BSC to incorporate:

a. responses to all TSC and HSE/ND queries (e.g. TQs and ROs) implemented in the body and listed in an annex of the BSC,

b. the basic justification for the 7300 cards. The justification of the cards appears from the document to be based from a sound original development process, although not to modern standards; however, its description is lacking in both detail and a supporting argument of proven in use, and

c. an explanation as to how the identified, applicable SAPs have been arrived at, with an indication of importance.

T15.TO1.14: In addition to addressing the main observations recorded above the designer or future operator / licensee is requested to address the individual observations in Section 3.6.3 of TSC Report (FNC37194-37352R), and update the DAS BSC and Westinghouse development procedures as appropriate.

Ovation and Displays (platform for DCIS (PLS and DDS))

The observation relating to Ovation Class 2/3 platform is presented in the TO1 observation below:

T15.TO1.01: The review of Ovation platform identified areas for improvement relating to the claims, arguments and evidence supporting the safety justification. The designer or future operator / licensee is requested to document claims, arguments and evidence to support the safety justification for the Ovation platform as a Class 2/3 nuclear safety system as part of a Basis of Safety Case .

SMART Sensors

The observation relating to SMART sensors is presented in the TO2 observation below:

T15.TO2.29: The use of SMART devices was reviewed as part of the main UK AP1000 C&I platform review. The designer or future operator / licensee is requested to complete the qualification of selected Class 1, 2 and 3 SMART devices in accordance with the Westinghouse process and to complete a SMART sensors checklist for each example.

OCS Class 1 Displays and Controls

The observation relating to OCS Class 1 Displays and Controls is presented in the TO2 observation below:

Annex 5

T15.TO2.36: The designer or future operator / licensee is requested to document the claims, arguments and evidence supporting the display panel and data amendment panel justification for the UK AP1000 OCS Class 1 Displays and Controls

Safety Assessment Principles

A review of conformance to the requirements of the HSE/ND Safety Assessment Principles (SAP) was conducted against Safety Case Maps and Basis of Safety Case documents provided by Westinghouse.

Review of Safety Case Maps

T15.TO1.09: The designer or future operator / licensee is requested to review the evidence presented in the Safety Case Maps and the relevant system BSC documents and ensure the points raised in the TO2s below are addressed:

T15.TO2.47: The review of EDR.2 SAP Safety Case Map in relation to the C&I platforms identified areas for improvement relating to the referenced evidence. The designer or future operator / licensee is requested to update the demonstration of SAP conformance, clearly identifying the following:

a. appropriately referenced evidence,

b. referenced documents, with their versions,

c. any diversity claims, arguments and evidence at the C&I platform level, and

d. any redundancy claims, arguments and evidence at the C&I platform level.

T15.TO2.48: The review of ESR.5 SAP Safety Case Map in relation to the C&I platforms identified areas for improvement relating to the referenced evidence. The designer or future operator / licensee is requested to update the demonstration of SAP conformance, addressing the following:

a. the clear identification of referenced documents, with their versions, and

b. resolution of mismatches between the level of compliance claimed in the SCM and the evidence cited; e.g. a requirements specification is cited as evidence that hardware and software are designed, manufactured and installed to appropriate standards.

T15.TO2.49: The review of EQU.1 SAP Safety Case Map in relation to the C&I platforms identified areas for improvement relating to the referenced evidence. The designer or future operator / licensee is requested to update the demonstration of SAP conformance, addressing the following:

a. the inclusion of argumentation and evidence that claims based on US Regulatory Guides and IEEE Standards that have been shown to be equivalent to in the UK,

b. the clear identification of referenced documents, with their versions,

Annex 5

c. identification of detailed evidence which addresses individual platforms (AC160, 7300 series equipment, CIM etc) and the modules within them, and

d. the inclusion of clear argumentation which shows how referenced evidence supports the claims and arguments.

T15.TO2.50: The review of ESS.21 SAP Safety Case Map in relation to the C&I platforms identified areas for improvement relating to the referenced evidence. The designer or future operator / licensee is requested to update the demonstration of SAP conformance, addressing the following:

a. produce demonstrations of SAP conformance for the CIM and DAS in addition to the PMS,

b. ensure that the reliability and diversity arguments are based on the currently proposed platforms,

c. the arguments for reliability should be made clear, with evidence supporting them; a justification of the complexity of the PMS and CIM should be produced which should include the effect on the reliability, and

d. it should be made clear how referenced evidence supports the claims and arguments for the platform.

T15.TO2.51: The review of ESS.27 SAP Safety Case Map in relation to the C&I platforms identified areas for improvement relating to the referenced evidence. The designer or future operator / licensee is requested to update the demonstration of SAP conformance, addressing the following:

a. the wording of the claims made do not always fully capture the intent of the SAP / each SAP paragraph and there is consequently doubt as to whether or not Westinghouse has claimed complete compliance with ESS.27; the Safety Case should clearly provide full coverage of all aspects of the SAP,

b. clearly identify the referenced documents with their versions for review,

c. identify the IEC Standards,

d. it should be made clear how referenced evidence supports the claims and arguments for the platforms,

e. compliance to standards should be under Production Excellence, not Compensating Measures,

f. if a claim of compliance with IEC 60880 is made the evidence should be referenced to support this, and

g. arguments and evidence should be identified to demonstrate compliance of the development tools with standards.

Annex 5

Review of Basis of Safety Case

T15.TO2.57: The review of AC160 platform identified areas for improvement relating to the adequacy of SAP conformance presented in the BSC. The designer or future operator / licensee is requested to update the demonstration of SAP conformance, addressing the following:

a. ESS.27

   i. The SAP conformance demonstration should clearly provide full coverage of all aspects of the SAP, to include clause 360a,

   ii. The demonstration of SAP conformance should be referenced explicitly and they should be consistent with each other, e.g. the SCM states that the suitability evaluation will be provided at a later date, where as the BSC cites a document which has not been written for the UK AP1000.

   iii. The referenced suitability evaluation should be for the UK AP1000.

   iv. In general, it should be made clear how referenced evidence supports the claims and arguments for the platform.

b. ESS.21

   i. Clause 355: The four points in this clause have not been clearly addressed with claims, arguments and evidence. It should be made clear how referenced evidence supports the claims and arguments for the platform,

   ii. Clause 356: The information provided does not identify unrevealed faults and how these relate to periodic surveillance tests. Identified unrevealed faults should be clearly documented.

c. EDR.2

   i. The PMS BSC does not address the required EDR.2 CAE trail.

d. EQU.1

   i. The PMS BSC does not address the required EQU.1 CAE trail.

T15.TO2.58: The review of CIM identified areas for improvement relating to the adequacy of the SAP conformance presented in the BSC. The designer or future operator / licensee is requested to update the demonstration of SAP conformance, addressing the following:

a. ESS.27

   i. The SAP conformance, presented in the BSC, should clearly provide full coverage of all aspects of the SAP in relation to the CIM platform. e.g. sub-clauses of clause 360 have not been addressed, gaps in the Production

Annex 5

Excellence have not been identified and Compensating Measures documented.

b. ESS.21

i. It is stated, in the ESS.21 section of the BSC, that the principles of ALARP have been considered when removing unnecessary complexity. Describe the methods used to reduce complexity,

ii. The claim against SAP clause 355 should be reviewed to determine its validity in the context of the CIM.

c. EQU.1

i. When arguing that tests have been conducted test results should be referenced.

ii. The SAP conformance, presented in the BSC should clearly provide full coverage of all aspects of the SAP in relation to the CIM platform. e.g. The EQU.1 section of the BSC has not demonstrated compliance with clause 165 of the SAP,

T15.TO2.59: The review of 7300 series equipment identified areas for improvement relating to the adequacy of the presented SAP conformance presented in the BSC. The designer or future operator / licensee is requested to update the demonstration of SAP conformance, addressing the following:

a. ESS.21

i. The SAP conformance, presented in the BSC should include a consideration of complexity.

ii. The SAP conformance, presented in the BSC should reference a fail safe analysis.

iii. The SAP conformance, presented in the BSC should include an analysis of how unrevealed faults relate to periodic surveillance tests.

iv. The SAP conformance, presented in the BSC should clearly provide full coverage of all aspects of the SAP in relation to the 7300 series equipment.

b. EDR.2

i. The SAP conformance, presented in the BSC should clearly provide evidence for adherence to SAP EDR.2 in relation to the 7300 series equipment platform, as the evidence presented relates to the application level.

c. EQU.1

Annex 5

i. The SAP conformance, presented in the BSC should clearly provide evidence for adherence to SAP EQU.1 in relation to the 7300 series equipment platform, as the evidence presented relates to the application level.

T15.TO1.15: In addition to addressing the main observations recorded above the designer or future operator / licensee is requested to address the individual observations in Section 3.4 and 3.5 of TSC Report (FNC37194-37352R), and update the demonstration of SAP conformance as appropriate.

Conclusion

Technical Observations have been assigned as TO1 or TO2, with TO1 having the higher significance.

Step 4 Task 15 has raised 14 TO1 observations and 54 TO2 observations.

The TSC review of the AC160 design submission (including the PMS BSC) concludes that the claims, arguments and evidence provided require improvement to support a demonstration that the requirements for a Class 1 system implementing Category A functions have been met. A number of observations have been raised by the TSC; the following being the emerging themes:

- the quality of documentation for QMS, Processes, Procedures and Planning (inc. configuration/change management) during and post Add Quality Demonstration,
- the completeness and application of Verification & Validation,
- the adequacy of the Basis of Safety Case document, and
- the provision of a suitability evaluation, descriptions of communications protocols and completeness of the Westinghouse's documentation set.

If, however, all of the observations raised by the TSC are adequately addressed, along with observations arising from a Westinghouse thorough review of the design submission, and adequate statistical testing and MALPAS analysis and independent verification are completed, it is the view of the TSC that nothing found to date precludes the AC160 from meeting the intent of appropriate guidance, including SAPs, TAGs and international standards requirements for a Class 1 system implementing Category A functions.

The TSC review of the CIM design submission concludes that the claims, arguments and evidence provided require improvement to support a demonstration that the requirements for a Class 1 system implementing Category A functions have been met. A number of observations have been raised by the TSC; the following being the emerging themes:

- the quality of documentation for QMS, Processes, Procedures and Planning (inc. configuration/change management),
- completeness and application of Verification and Validation and requirements traceability, and

Annex 5

- the adequacy of the CIM BSC, substantiation of reliability targets, and adequacy of overall CIM documentation.

If, however, all of the observations raised by the TSC are adequately addressed, along with observations arising from Westinghouse's own thorough review of the design submission, it is the view of the TSC that nothing found to date precludes the CIM from meeting the intent of appropriate guidance, including SAPs, TAGs and international standards, requirements for a Class 1 system implementing Category A functions.

The TSC review of the 7300 series equipment design submission concludes that the claims, arguments and evidence provided require improvement to support a demonstration that the requirements for a Class 2 system implementing Category A functions have been met. A number of observations have been raised by the TSC; the following being the emerging themes:

- the quality of documentation for QMS, Processes, Procedures and Planning (inc. configuration/change management),
- completeness and application of Verification and Validation, and
- the adequacy of the DAS BSC.

If, however, all of the observations raised by the TSC are adequately addressed, along with observations arising from Westinghouse's own thorough review of the design submission, it is the view of the TSC that nothing found to date precludes the DAS from meeting the intent of appropriate guidance, including SAPs, TAGs and international standards, requirements for a Class 2 system implementing Category A functions.

The TSC review of the Ovation and Displays (forming the DCIS) submission concludes that the platform functionality descriptions and claims, arguments and evidence provided require improvement to support a demonstration that the requirements for a Class 2/3 system implementing Category B/C functions have been met. A number of observations have been raised by the TSC; the following being the emerging theme:

- provision of identified evidence in support of the high level claims and it's availability for review.

If, however, all of the observations raised by the TSC are adequately addressed, along with observations arising from a Westinghouse thorough review of the design submission, then the Ovation application could be demonstrated to meet the requirements for a Class 2/3 system implementing Category B/C functions.

The TSC review of the SMART sensors submission concludes that the Westinghouse approach to justification of SMART devices is in principle acceptable. A number of low priority observations have been raised by the TSC; the following being the most significant:

- completion of examples of the application of Westinghouse's chosen approach to justification of SMART devices in UK AP1000, and
- completion of a the SMART sensors checklist for the specific devices above.

Annex 5

If, however, all of the observations raised by the TSC are adequately addressed, along with observations arising from a Westinghouse thorough review of the design submission, then the SMART sensors could be demonstrated to meet the requirements for Class 1, 2 and 3 systems implementing Category A, B and C safety functions.

The TSC reviews of the Safety Case Maps and BSC SAP submissions conclude that the evidence cited in these documents requires improvement to align with the claims and arguments.

The designer or future operator / licensee is requested to consider the wider implications when addressing the observations and not to simply focus on the particular observations identified, as this review has been undertaken on a sampling basis.

The TSC concludes that a positive outcome from this review could be achieved should the designer or future operator / licensee adequately address all observations identified in the report.

References

1 Observations from GDA Step 4 Supporting Review Activities, FNC37194-66584V, Output of Stonehouse 2 Review of WEC, FNC37194-66584V[7] Annex A

2 Observations from GDA Step 4 Supporting Review Activities, FNC37194-66584V, Minutes of meeting at Stonehouse 3 on 17 & 18 Jan 2011, Annex K

[7] ND Note: Observations from GDA Step 4 Supporting Review Activities, FNC37194-66584V. Issue 1.0. 25 July 2011. TRIM Ref. 2011/420512.

Annex 6

TSC Task Summary - Review of the C&I Systems Important to Safety [8]

Note this information has been imported from a TSC report (Ref. 73) and the formatting of the TSC report has been retained.

This Annex refers to the Pre-Construction Safety Report (PCSR) and European Design Control Document (DCD), which are references to the:

> AP1000 Pre-construction Safety Report, UKP-GW-GL-732 Revision 2, Westinghouse Electric Company LLC, December 2009, (Ref. 22); and
>
> AP1000 European Design Control Document, EPS-GW-GL-700 Revision 1, Westinghouse Electric Company LLC, December 2009, (Ref. 27);

respectively.

The versions of the BSCs referred to in this Annex are:

> PMS UKP-PMS-GLR-001 Rev 0 November 2010 (Ref. 49).
>
> CIM UKP-PMS-GLR-002 Rev 0 November 2010 (Ref 98).
>
> DAS UKP-DAS-GLR-001 Rev 0 November 2010 (Ref. 50).

[8] Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 6

Annex: TSC Task Summary: Review of the C&I Systems Important to Safety – AP1000

This Annex summarises a review of the Control and Instrumentation (C&I) Systems Important to Safety (Class 1, 2 and 3 systems) for the Westinghouse UK AP1000 reactor design. The review was undertaken in Step 4 of GDA by a Technical Support Contractor (TSC) in support of the HSE / ND. This review has considered issues relating to the overall C&I systems, often called applications, and the lifecycle of application software. A separate TSC review has examined the issues specific to platforms and pre-developed equipment.

The claims and argumentation presented by Westinghouse were reviewed in the preceding Step 3. The aim of this Step 4 review has been to gain confidence that Westinghouse as the Requesting Party (RP) has adequate evidence to support the claims and argumentation relating to the conformance/compliance of C&I systems to appropriate guidance and standards. These include relevant HSE / ND Safety Assessment Principles (SAPs), Technical Assessment Guides (TAGs) and international Nuclear Sector Standards. This review of evidence has been carried out on a sampling basis.

The UK AP1000 C&I systems are defined in Chapter 6.7 of the UK AP1000 Pre-Construction Safety Report (PCSR) and Chapter 7 of the European Design Control Document (EDCD). The C&I systems included in this review are:

- The Protection and Safety Monitoring System (PMS), used as the primary protection system,
- The Diverse Actuation System (DAS), used as the secondary protection system,
- The Plant Control System (PLS) including the Data Display and Processing System (DDS) used for the control and monitoring system forming the Distributed Control and Information System (DCIS).

A sampling approach was used to review the Westinghouse identified evidence in the GDA Step 4 process. The initial sample of evidence reviewed by the TSC indicated that the Westinghouse UK AP1000 PCSR and supporting documentation required improvements. The HSE/ND and TSC undertook considerable additional work to provide Westinghouse with feedback on the improvements required to provide suitable documents for GDA. These improvements were required to provide a clear Claims, Arguments and Evidence (CAE) trail to support the demonstration of the adequacy of the safety and safety-related equipment. This required Westinghouse to supplement existing documentation, which focussed on equipment performance and functions, with documentation setting out the supporting Safety Case.

In response to the feedback, Westinghouse revised its primary documentation set and provided documents more suitable for review purposes. This included the creation of separate Basis of Safety Case (BSC) documents by Westinghouse for the PMS, Component Interface Module (CIM) and DAS. Westinghouse has agreed to provide a BSC for PLS/DDS but this was not available within the timeframe of GDA Step 4 review.

As a result, the review of Step 4 C&I systems important to safety is based on the following specific areas:

Annex 6

- Consideration of responses to Observations identified in the HSE / ND Step 2 and Step 3 C&I Assessment Reports,
- Consideration of responses to technical observations from the TSC Step 3 report on C&I systems important to safety,
- Review of Westinghouse responses to Technical Queries (TQ) and Regulatory Observations (RO) raised during Step 3 and Step 4,
- Review of Westinghouse CAE submissions to consider conformance with a sample of HSE/ND Safety Assessment Principles (SAPs):
    - ESS.27 Computer Based Safety Systems,
    - ESS.21 Reliability,
    - ESR.5 Standards for Computer-Based Equipment,
    - EQU.1 Qualification Procedures,
    - EDR.2 Redundancy, Diversity and Segregation.
- Review of a deep slice sample of Westinghouse CAE submissions to consider compliance with agreed international Nuclear Sector Standards:
    - IEC61513,
    - IEC60880,
    - IEC62138,
    - IEC60987.
- Review of Westinghouse CAE submissions relating to complex, calculated trips.

Westinghouse has provided the HSE / ND with letter UN REG WEC 000475 that identifies the status of the lifecycle phases for each of the systems important to safety available to the TSC during the period of the GDA review process. Key points noted from this letter include:

- All systems: For “design”, “implementation” and “test” phases the review is limited to the processes guiding these phases as the outputs from the phases are not available,
- PMS: Processes for and outputs from the “design requirements” and “system definition” phases are available and consequently the review concentrates on outputs,
- DAS: The output from “design requirements” and “system definition” phases are not complete,
- PLS and DDS: The output from the “system definition” phase is not complete.

During the course of the Step 4 review, Westinghouse changed the DAS platform and architecture in response to the Regulatory Observations; RO-AP1000-081 and RO-AP1000-071 raised by HSE/ND. As introduced above, although Westinghouse declared the outputs from all phases of the DAS design lifecycle out of scope of their GDA submission, this review identifies Technical Observations relating to the processes applicable to the lifecycle phases (which are generally in scope of GDA) and, where available, suitably mature evidence.

Annex 6

The application programming of the complex hardware for the PMS CIM was originally included in the scope of this review; this is now covered as a component of the PMS in the TSC Review of Platforms and Pre-developed Equipment. A new interlock/blocker has been introduced by Westinghouse during Step 4 as a design change arising from RO-AP1000-082 raised by HSE / ND. This is covered in the TSC Review of System-Level Architecture.

In addition to the Step 2 and 3 HSE / ND Observations, other TSC observations have been considered by raising Technical Queries with Westinghouse that have been addressed in Step 4. As identified below, TQs and observations that have not been satisfactorily addressed have been merged into a single set of Technical Observations by the TSC that address specific system related topics.

A total of 42 technical observations have been raised, these observations have been designated as TO1 or TO2 by the TSC depending on their significance, of which TO1 is the higher. Six of these observations have been designated as TO1 and 36 observations have been designated as TO2. Where it is judged that a sufficient number of TO2s have been identified on a topic, a single TO1 is used to provide focus on the topic.

The technical observations are listed with respect to the specific C&I systems important to safety.

Protection and Safety Monitoring System (PMS)

T16.TO1.01: The review of the Westinghouse submissions related to the PMS concluded that the CAE provided require further improvement to demonstrate that PMS satisfies Class 1, Category A requirements. The designer or future operator / licensee is requested to produce an update to the PMS Basis of Safety Case (BSC) document to address the TO2s linked to this TO1, as follows:

T16.TO2.01: It is understood from the letter UN REG WEC 000424 that Westinghouse has committed to undertaking a complete and independent assessment of the UK AP1000 PMS BSC. The letter states 'the third party review of the PMS BSC will be a review of the arguments and evidence justifying that the PMS is fit for purpose for a Class 1 safety system performing automatic reactor trip and ESFAS '(Engineered Safety Features Actuation System)' functions with a reliability claim of 1E-3 failures per demand'. However, it is not clear whether Westinghouse is considering this review to be an Independent Confidence Building Measure (ICBM) or as part of Production Excellence (PE). The designer or future operator / licensee is requested to explain and document the role of this review in the context of SAP ESS.27 requirements for ICBM and PE.

T16.TO2.02: The Deviation Matrix (which tracks areas for improvement for compliance with IEC nuclear standards) is not currently referenced from the PMS BSC. The designer or future operator / licensee is requested to reference and / or include the Deviation Matrix in the BSC and record the resolution of open Deviation Matrix items.

T16.TO2.03: The PMS BSC lists a number of commitments / requirements for post GDA activities. The designer or future operator / licensee is requested to update the safety plan to include these commitments and ensure that they are tracked and implemented.

T16.TO2.04: The PMS BSC does not clearly define the safety principles and standards that Westinghouse has adopted for the development of the PMS, or information on how these safety principles and standards have been fulfilled. The designer or future operator / licensee is requested to update the PMS BSC to ensure that it identifies the safety principles and standards adopted for the PMS. In addition, the updated PMS BSC should describe how these safety

Annex 6

principles and standards are fulfilled with respect to appropriate company safety processes, SAP s and good practice as presented in the appropriate IEC Standards.

T16.T02.05: The PMS BSC makes reference to the Safety Case Maps (SCM) and clause by clause standards review work to support claims and arguments that the requirements of the relevant SAP and IEC Standards have been fulfilled. The PMS BSC also makes claims in support of conformance with SAP ESS.21. However, the review of the PMS BSC has found that there are areas for improvement regarding the CAE supporting conformance with relevant SAPs and compliance with relevant IEC Standards. The designer or future operator / licensee is requested to:

a. Update the BSC to demonstrate that the PMS meets the requirements of the SAPs and relevant IEC Standards and to address the specific areas for improvement identified in this review through sampling (identified in T16.T02.29, T16.T02.30, T16.T02.39, T16.T02.40, T16.T02.04 and T16.T02.01),

b. Update all relevant demonstrations of SAP conformance and IEC Standards compliance.

There are a number of observations made against the PMS BSC Rev. 0 (November 2010), which are relevant to both the system (application) and platform. These are all tracked in the TSC report 37194-37352R (Platforms and Pre-developed Equipment) by a technical observation (T15.T02.63).

T16.T02.06: The designer or future operator / licensee is requested to produce an updated PMS BSC to ensure that full and comprehensive information is provided for the following areas relating to the development processes including:

a. Detailed documentation describing how the PMS application software is placed under configuration control and the processes followed to control changes,

b. Ensure the PMS test procedures are identified in the BSC and demonstrate how these comply with appropriate IEC Standards,

c. Confirmation and demonstration that a suitable tool evaluation process exists, and that evaluations are carried out and documented as described in the development process,

d. Document application level test and source code analysis coverage and confirmation that statistics are recorded,

e. Document the processes and procedures used for both assessment and use of the requirements management tools.

T16.T02.10: The designer or future operator / licensee is requested to produce an update to the PMS BSC to ensure that the following areas for improvement relating to IEC Standards compliance are addressed:

a. Reference the compliance matrices (which form an important reference for the Safety Case) as controlled documents with a document number and revision,

b. Clearly identify the content of the referenced standards compliance matrices e.g column headings for the clause by clause compliance matrix for IEC 61513 are accurate,

c. Identify clear and concise CAE trails within the compliance matrices,

d. Differentiate between full and partial compliance to individual standard clauses; providing a justification for gaps,

Annex 6

e. Regarding the deep sample areas performed by the TSC for IEC 61513. The designer or future operator / licensee is requested to substantiate that the requirements specification for the PMS is addressed (section 6.1.1 of IEC 61513).

f. Ensure the IEC 60880 compliance matrix is updated to include all applicable clauses and present detailed design, implementation and verification evidence, when available,

g. Produce a substantiation for any inputs to the PMS from other C&I systems that are used to perform Category A functions.

T16.T02.47: During the review of the C&I systems important to safety, an observation has been made relating to the selection of automatic and manual actuation of the PMS safety functions. The designer or future operator / licensee is requested to demonstrate conformance to SAPs ESS.8 and ESS.9, in particular, explaining the rationale for the selection of automatic versus manual actuation of safety functions.

T16.T01.02: During the review of the C&I systems important to safety, observations have been made that relate to the claims made in the PMS BSC that statistical testing is used to substantiate the reliability claim on the PMS and as a Compensating Measure for the qualification of complex devices used in the PMS. The designer or future operator / licensee is requested to:

a. Produce a substantiation for the claim that statistical testing is a Compensating Measure and an Independent Confidence Building activity,

b. Produce a substantiation for the validity of the approach to statistical testing, i.e. applicable to a single division, given the lack of symmetry between the four PMS divisions,

c. Produce a substantiation for the planned approach to derivation of the PMS reliability based on the statistical testing results, given the lack of symmetry between the four PMS divisions,

d. Produce a substantiation for statistical testing and MALPAS analysis for the PMS, in accordance with the high-level planning information already provided, and demonstrate that the testing and analysis will be completed in accordance with the plans, and be independently verified and validated,

e. Clarify which clause of ESS.27 the MALPAS analysis is to address and produce a justification for the use of MALPAS for this approach.

T16.T02.07: It has been identified in the DCD that in some cases, the PMS is not completely four-way redundant and hence some of the PMS functionality is provided in fewer than four divisions. In this context, the designer or future operator / licensee is requested to:

a. Identify exactly what features and functions in the PMS are not completely four-way redundant and how this impacts on the reliability analyses,

b. Substantiate the adequacy of provision for the level of redundancy implemented,

c. Produce a demonstration of the maintenance and test procedures and how they maximise availability and operability based on the reduced level of redundancy.

T16.T02.08: During the review of the C&I systems important to safety, observations have been made that relate to the implementation of complex, calculated trips within the PMS. A checklist based on SAPs, TAGs and IEC Standards was issued to the RP and a response received. It is understood that the level of response to this checklist reflects the immaturity of the design, and that the checklist requests information that may not be available until the implementation. In addition, a review of a complex 'PC Element' was conducted resulting in observations relating to the documented analysis. In recognition

Annex 6

of these, the designer or future operator / licensee is requested to produce documentation to substantiate the complex calculated trips checklist once the information is available, based on the responses requested in the checklist. It is also requested that the designer or future operator / licensee document a re-evaluation of the analysis of the 'PC Elements'.

T16.T02.09: During the review of the C&I systems important to safety, observations have been made that relate to the loading effects on the PMS (in particular, relating to the PMS processor and its communications) that could lead to unforeseen failure modes. The designer or future operator / licensee is requested to produce a substantiation[9] that loading effects cannot lead to unmanaged failure modes. This could for example be claimed based on deterministic behaviour and demonstrated by analysis and / or testing.

Where future testing is being used as part of the substantiation, the designer or future operator / licensee is requested to ensure that a test planning document is produced to support this activity.

T16.T02.45: It is understood that manual actuations of permissives, blocks, resets and system level resets originate at the QDPS (Qualified Data Processing System) /Safety Display as soft controls. The designer or future operator / licensee is requested to substantiate that failure of these soft controls could not lead to an unsafe, unexpected operation of the automatic operation of the PMS.

T16.T02.42: During the review of the C&I systems important to safety, observations have been made that relate to the operational behaviour of the PMS. The designer or future operator / licensee is requested to:

a. Substantiate that the operational behaviour of the PMS is deterministic and changes of state during normal operation (i.e. not including state changes which are brought about by an internal failure) are only dependent on the external influences (e.g. signals from other systems, sensors or operator actions) that are relevant and significant to the condition to which the PMS is responding,

b. Produce a plan to demonstrate how these PMS states will be adequately tested so that, when implemented, risk to correct operation will be minimised.

The TSC review of the CIM design submission was carried out in the TSC report 37194-37352R (*Platforms and Pre-developed Equipment*). No further observations or conclusions are made here.

If all of the Technical Observations raised by the TSC are adequately addressed, along with issues arising from a thorough review of the design submission by the designer or future operator/licensee, it is the view of the TSC that there have been no findings to preclude the PMS from meeting the intent of appropriate guidance and standards including SAPs, TAGs and international standards, for a Category A, Class 1 system.

Diverse Actuation System (DAS)

T16.T01.03: The DAS design is not complete and following changes to its platform and architecture, the TSC review of the DAS design submission is principally based on the DAS BSC. The review

[9] ND clarification: the substantiation should be included in or referenced from the BSC.

Annex 6

concludes that the CAE provided in the DAS BSC require further improvement to demonstrate that DAS satisfies the requirements of a Category A, Class 2 system.

The designer or future operator / licensee is requested to produce an update to the DAS Basis of Safety Case (BSC) document to address the TO2s linked to this TO1, as follows:

T16.TO2.11: The DAS BSC does not clearly define the safety principles and standards that Westinghouse has adopted for the development of the DAS, or information on how these safety principles and standards have been fulfilled. The designer or future operator / licensee is requested to update the DAS BSC to ensure that it identifies the safety principles and standards adopted for the DAS. In addition, the updated DAS BSC should describe how these safety principles and standards are fulfilled with respect to appropriate company safety processes, SAP s and good practice as presented in the appropriate IEC Standards.

T16.TO2.12: The DAS BSC does not currently state why it is considered that the DAS application is fit for purpose. The designer or future operator / licensee is requested to produce an update to the DAS BSC so that the document contains sufficient and adequate information to substantiate that the DAS is fit for purpose.

T16.TO2.13: The DAS BSC is not currently supported by a detailed clause by clause analysis demonstrating compliance of processes with the requirements of IEC 61513; Nuclear power plants – Instrumentation and control for systems important to safety - General requirements for systems. The designer or future operator / licensee is requested to ensure clause by clause standards compliance work for the DAS is produced and referenced from the DAS BSC.

T16.TO2.15: The designer or future operator / licensee is requested to produce an updated DAS BSC to ensure that it adequately substantiates conformance with all relevant SAPs. Based on a sampling approach for the SAPs, areas for improvement have been noted as follows:

a. SAP ESS.21 (Reliability) has a response provided in the BSC. However, there is scope for improvement in the following areas, including:

   i. Substantiate how the complexity of the DAS is justified to meet the reliability requirements,

   ii. Demonstrate how unrevealed faults are identified and periodic tests can be applied,

   iii. Substantiate how the voting mechanism provides the required level of safety and reliability.

b. SAP EDR.2 (Redundancy, Diversity and Segregation) has a response provided in the BSC. However, there is scope for improvement in the following areas, including:

   i. Produce a justification of the voting system adopted in the context of redundancy, diversity and segregation,

   ii. Produce a justification of any specific internal segregation requirements and methods of implementation,

c. SAP EQU.1 (Qualification procedures) has a response provided in the BSC. However, there is scope for improvement, for example, the SAP should reference the document APP-GW-G1-002 Rev 1 (AP1000 Plant Equipment Qualification Methodology),

d. SAP ESS.22 (Avoidance of Spurious Operation) has a response provided in the BSC. The response does not mention a systematic assessment of fault sequences, and

Annex 6

substantiation that the reliability of the defences against spurious actuation are commensurate with the risks should the DAS spuriously actuate,

There are a number of observations made against the latest revision of the DAS BSC, which are relevant to the system (application) and platform level. These are all tracked in the TSC report 37194-37352R (Platforms and Pre-developed Equipment) as T15.TO2.64.

T16.TO2.17: The designer or future operator / licensee is requested to address the following observations relating to test and maintenance and produce a substantiation of adequacy in the updated DAS BSC:

a. Substantiation that the proposed architecture permits a channel to be taken out of service for test and / or maintenance and the DAS will still meet its intended reliability target,

b. Demonstration that the six monthly testing of the DAS is consistent with the proof test frequency necessary to meet the reliability targets for the DAS.

T16.TO2.48: During the review of the C&I systems important to safety, an observation has been made relating to the selection of automatic and manual actuation of the DAS safety functions. The designer or future operator / licensee is requested to demonstrate conformance to SAP ESS.8, in particular, explaining the rationale for the selection of automatic versus manual actuation of safety functions.

T16.TO2.43: During the review of the C&I systems important to safety, observations have been made that relate to the operational behaviour of the DAS. The designer or future operator / licensee is requested to:

a. Produce a substantiation that the operational behaviour of the DAS is deterministic and changes of state during normal operation (i.e. not including state changes which are brought about by an internal failure) are only dependent on the external influences (e.g. signals from other systems, sensors or operator actions) that are relevant and significant to the condition to which the DAS is responding,

b. Produce a plan to demonstrate how these DAS states will be adequately tested so that, when implemented, correct operation will be ensured.

T16.TO1.04: During the review of the C&I systems important to safety, observations have been made that relate to the adequacy of the DAS architecture as detailed in RO-AP1000-071. The designer or future operator/licensee is requested to demonstrate how the preferred failure modes are determined and the detailed design shows how this is achieved,

If all of the Technical Observations raised by the TSC are adequately addressed, along with issues arising from a thorough review of the design submission by Westinghouse, it is the view of the TSC that there have been no findings to preclude the DAS from meeting the intent of appropriate guidance and standards including SAPs, TAGs and international standards, for a Category A, Class 2 system.

The Distributed Control and Information System (DCIS) including the Plant Control System (PLS) and Data Display and Processing System (DDS)

T16.TO1.05: The review of the PLS/DDS submission (including the responses to RO-AP1000-078 and 080) concludes that in addition to the system, architecture and functionality descriptions, the CAE provided requires improvement to support the PLS/DDS Category B/C, Class 2/3 safety requirements.

Annex 6

To consolidate the above, the designer or future operator / licensee is requested to produce a PLS/DDS BSC document that includes addressing the TO2s linked to this TO1, as follows:

T16.TO2.19: The PLS/DDS BSC should provide a clear statement defining the safety requirements of the system, and demonstrate that the system meets those requirements.

T16.TO2.21: The PLS/DDS BSC should demonstrate compliance with the applicable key IEC nuclear sector standards, for example, by production of an adequate clause by clause compliance matrix for each of the standards. The compliance matrices should be referenced from the BSC document. The designer or future operator / licensee is requested to address the following areas when compiling the PLS/DDS BSC:

a. As the compliance matrices form an important reference for the Safety Case, these should be controlled documents, with a document number and revision number,

b. All IEC Standards clauses should be documented with claim, arguments and evidence. Examples of where there is scope for improvement:

   i. Produce an update of the clause by clause compliance demonstration for IEC 61513; currently very little reference is made to the DCIS design and implementation process, compared with its usefulness as a document describing the lifecycle,

   ii. Produce a clause by clause compliance demonstration for the PLS / DDS for IEC 62138,

   iii. Produce an update of the clause by clause demonstration for IEC 60987; currently an adequate claim is made with respect to clauses (10.5 to 10.7) relating to Electromagnetic Compatibility (EMC); however, there is no CAE presented with respect to any of the other areas of IEC 60987.

c. Demonstrate compliance with the applicable key IEC nuclear sector standards and ensure that the documentation reflects and substantiates (through the arguments and evidence cited) this level of compliance, and that all areas of non-compliance or partial compliance are identified and justified,

d. Document the arguments linking each IEC Standard clause claim to the cited evidence. Where a claim is made, the evidence is often difficult to trace due to the lack of an argument explaining how compliance is achieved and where that is documented in the evidence.

T16.TO2.22: The designer or future operator / licensee is requested to demonstrate in the PLS/DDS BSC conformance with the applicable SAPs, in doing so the following observations should be addressed:

a. SAP ESS.27 (Computer-based safety systems) applies because the PLS, although a safety-related system, is classed as “complex”. With respect to the response to RO-AP1000-080, the designer or future operator / licensee is requested to clarify and substantiate the claims of Production Excellence for the PLS/DDS. In addition, produce a demonstration for the Independent Confidence Building activities that will be applied the PLS/DDS,

b. Some examples of SAPs are provided below; however, the designer or future operator / licensee is requested to demonstrate conformance with all applicable SAPs:

   i. SAP ESR.9 (Response of control systems to normal plant disturbances); Produce a demonstration that the PLS/DDS responds in a timely and stable manner to normal plant disturbances without causing demands on safety systems,

Annex 6

ii. SAP ESR.3 (Provision of controls); Demonstrate adequate and reliable controls are provided to maintain variables within specified ranges,

iii. SAP EDR.2 (Redundancy, diversity and segregation); Substantiate the segregation and separation of equipment provided, substantiating why the approach is suitable,

iv. SAP EMT.7 (Functional testing); Substantiate the provisions for maintenance and test.

T16.T02.23: The designer or future operator / licensee is requested to produce a demonstration of the adequacy with respect to SAPs and relevant IEC Standards regarding the use of PCs (Personal Computers) and Commercial Off The Shelf (COTS) operating system(s) for implementation of the PLS/DDS.

T16.T02.20: The designer or future operator / licensee is requested to demonstrate that a suitable tool evaluation process exists for the PLS/DDS, and that evaluations are carried out and documented as described in the process. As part of this, the designer or future operator / licensee is requested to substantiate the adequacy of the Westinghouse Application Builder tool for use in safety-related systems.

T16.T02.24: The designer or future operator / licensee is requested to substantiate that communications are capable of meeting the overall performance requirements specifications for the PLS/DDS, under all plant demand (normal and fault) conditions. If this is to be achieved by future analysis or testing, the designer or future operator / licensee is requested to document coverage in the appropriate planning documents.

T16.T02.25: The designer or future operator / licensee is requested to produce a demonstration that Common Cause Failures / Common Mode Failures and dependent failures have been considered and minimised for the PLS/DDS. In accordance with an appropriate standard such as IEC 62340.

T16.T02.26: The designer or future operator / licensee is requested to substantiate in the BSC document, the adequacy of the controls in place to ensure only correct updates are made via the permanently connected engineering workstations and database server.

T16.T02.27: The designer or future operator / licensee is requested to document in the BSC the qualification and development processes history of the Application Builder Tool.

If all of the Technical Observations raised by the TSC are adequately addressed, along with issues arising from a thorough review of the design submission by Westinghouse, it is the view of the TSC that there have been no findings to preclude the PLS/DDS from meeting the intent of appropriate guidance and standards including SAPs, TAGs and international standards, for a Category B/C, Class 2/3 system.

Generic observations relating to C&I systems important to safety

T16.T02.28: During the review of the C&I systems important to safety, observations have been made that relate to document control. The designer or future operator / licensee is requested to substantiate the claim that a robust document control system is in place and that consequently the documents reviewed and in use for the UK AP1000 are the most recent applicable documents.

T16.T02.38: The designer or future operator / licensee is requested to explain how the failure modes for the ESFAS (covering PMS and DAS actuation) were identified, and to substantiate the adequacy of the approach to selection and the outcome.

Annex 6

Observations relating to the review of the Safety Case Map (SCM) submissions

T16.T01.06: The designer or future operator / licensee is requested to review the evidence presented in the SCMs and the relevant system BSC documents and to produce an adequate demonstration of conformance to HSE/ND SAP to address the points raised in the following TO2s:

T16.T02.29: The review of ESS.27 SAP SCM in relation to the C&I systems important to safety identified areas of improvement relating to the referenced evidence. The designer or future operator / licensee is requested to update the ESS.27 SAP conformance demonstration, addressing the following:

a. The claim of Production Excellence needs to be fully and clearly supported, providing a clear CAE structure covering all relevant IEC Standards,

b. The claim of Independent Confidence Building Measures needs to be fully and clearly supported, providing a clear CAE structure covering all aspects of SAP paragraph 361. Adequate responses to T16.T01.02 and T16.T02.01 are relevant to this observation,

c. The claim regarding compensatory activities needs to be clarified, i.e. have weaknesses been identified in the production processes that require compensatory activities to be claimed? Details of any Compensating Measures claimed should be referenced,

d. Evidence needs to be provided with respect to the PLS/DDS,

e. The structure of the SCM is an area for improvement, as follows:

i. To enable a full and complete review of the SCM, the designer or future operator/licensee is requested to make available all evidence identified on the SCM in support of claims and arguments,

ii. The CAE trails are very complex and contain considerable redundant information, e.g. complex claims regarding compliance with IEEE standards under “Production Excellence”,

iii. Many of the CAE trails are unclear e.g. the claim for “Compensatory Activities” begins with the claim “No weaknesses in production processes” but then has the sub-claim “There are compensatory measures to address any gaps in production excellence” which does not follow on logically from the higher level claim,

iv. It is often unclear how referenced evidence supports the claims and arguments. For example, the claim for production excellence is supported by reference to a planning document which identifies IEEE standards. It is therefore unclear how this cited evidence supports the claim of production excellence in a UK regulatory regime, expecting compliance to IEC Standards,

v. Lack of revision status of the identified evidence on the SCM,

vi. The CAE is characterised by a misunderstanding of the requirements of the SAP, for example, under Independent Confidence Building Measures, CAE cited relates to normal design review, test, V&V etc. that is carried out as part of the development process. Whilst this is relevant to production excellence it is not considered independent in the context of Independent Confidence Building Measures. The Safety Case supporting ESS.27 should be updated to correctly identify the activities and therefore CAE in support of the three clauses (and sub-clauses) of the SAP.

Annex 6

T16.T02.30: The review of EDR.2 SAP SCM in relation to the C&I systems important to safety identified areas of improvement relating to the referenced evidence. The designer or future operator / licensee is requested to update the EDR.2 SAP conformance demonstration, addressing the following:

a. The identified evidence should fully support the claim regarding redundancy within the PMS. For example, the claim states "PMS – 4 redundant divisions" however the identified evidence indicates that the PMS is not wholly 4-way redundant as some functionality is provided in fewer than four divisions. See also T16.T02.07,

b. The CAE regarding internal redundancy of the DAS and PLS/DDS should be identified in an updated demonstration of SAP conformance. The SCM currently only identifies the CAE for the Nuclear Steam Supply System (NSSS) Controllers and cabling. The redundancy internal to the three systems should be demonstrated to be adequate,

c. An updated demonstration of SAP conformance should clearly show how the redundancy requirements were developed for each system,

d. An updated demonstration of SAP conformance should clearly state how the claim of independence within a PMS division is supported,

e. An updated demonstration of SAP conformance should clearly show how segregation is achieved both within the systems (PMS, DAS & PLS / DDS) and between the systems,

f. An updated demonstration of the SAP conformance should identify the appropriate standards,

g. In addition, the review is complicated by the structure / content of the SCM. the designer or future operator/licensee is requested to:

   i. Make available all evidence identified on the SCM in support of a claim,

   ii. Identify the revision status of the referenced evidence when updating the demonstration of SAP conformance.

T16.T02.39: The review of ESR.5 SAP SCM in relation to the C&I systems important to safety identified areas of improvement relating to the referenced evidence. The designer or future operator / licensee is requested to update the ESR.5 SAP conformance demonstration, addressing the following:

a. The SCM covers IEC 61513, 62138 and 60987 only. The SCM should also provide CAE with respect to lower level standards,

b. The evidence documents (i.e. the compliance matrices) should be referred to in a less ambiguous way. The designer or future operator / licensee is requested to make the clause by clause compliance matrices controlled documents with a document number and revision:

   i. T16.T02.10 covers observations relating to the Standards compliance demonstration for the PMS. The designer or future operator / licensee is requested to adequately respond to this TO as an integral part of the demonstration of conformance for SAP ESR.5,

   ii. T16.T02.21 covers observations relating to the Standards compliance demonstration for PLS/DDS. The designer or future operator / licensee is requested to adequately respond to this TO as an integral part of the demonstration of conformance for SAP ESR.5.

Annex 6

T16.T02.40: The review of ESS.21 SAP SCM in relation to the C&I systems important to safety identified areas of improvement relating to the referenced evidence. The designer or future operator / licensee is requested to update the ESS.21 SAP conformance demonstration, addressing the following:

a. The DAS is not adequately covered by the SCM. The DAS section of the ESS.21 SCM is not reviewed as the sub-claims and evidence do not appear to be relevant to the current design of DAS or to the requirements of the SAP, the SCM should be updated to include the current DAS design,

b. The SCM should include reference to PLS/DDS,

c. The CIM and PMS both contain complex hardware, the designer or future operator / licensee is requested to produce a justification for the claim that clause 355 of ESS.21 is not considered to be applicable.

d. For most of the claims, there are no arguments presented, e.g. the claim is “safety system not overly complex” and the evidence is the architecture drawings. An argument is required to explain to the reader how the architecture drawings demonstrate that the safety system is not overly complex,

e. The evidence in context of the claim is difficult to trace in places. For example, under the claim “fail safe”, the RP has identified a list of ten evidence documents which are then cited for all sub-claims whereas in reality, different documents support the different sub-claims,

f. With respect to the claim “fail safe”, the designer or future operator / licensee is requested to clarify the claims regarding operation of Passive Residual Heat Removal Heat Exchanger (PRHR HX), Core Make-up Tank (CMT), Passive Containment Cooling System (PCS) and containment isolation features under fault conditions, and in particular their susceptibility to spurious operation of the CIM,

g. The SAP text states "incorporate the means of revealing internal faults from the time of their occurrence"; however, the SCM shows as a sub-claim to this “periodic surveillances provides assurance that the safety functions are operable”. Periodic testing will only reveal faults at the time of the test, not from the time of the fault's occurrence. The designer or future operator / licensee is requested to resolve (or justify) this discrepancy, for example by demonstrating conformance to SAP paragraph 356.

T16.T02.44: The review of EQU.1 SAP SCM in relation to the C&I systems important to safety identified areas of improvement relating to the referenced evidence. The designer or future operator / licensee is requested to update the EQU.1 SAP conformance demonstration, addressing the following:

a. The SCM should indicate clearly whether the CAE is relevant to both platform and application,

b. The SCM should demonstrate how the C&I system requirements are broken down into the subsystem requirements to allow, for example, verification by testing of the individual subsystems,

c. The structure / content of the SCM should be made clear and complete by ensuring the following are addressed in the next release:

Annex 6

i. Each referenced piece of evidence should be uniquely identified with a revision status,

ii. The pertinent section of a particular piece of referenced evidence should be identified, along with a clear argument explaining it's relevance,

iii. All documents should be available for review to allow a complete review of the SCM evidence,

iv. Discussions provided in other Westinghouse documentation that are pertinent to this observation should be made coherent with the argumentation and evidence referenced in this SCM.

In addition, the designer or future operator / licensee is requested to produce a demonstration of the process and procedures that were used to generate the test plan and the detail within the plan, including the traceability between the requirements specification, the test plan and the exact test specifications.

This document records a review of the Westinghouse submission for a sample of the systems important to safety against selected SAPs, guidance and international Nuclear Sector Standards. The review raised 6 TO1s and 36 TO2s. These are listed above and should be treated as part of the conclusions for each system.

The Safety Case for the use of the PMS as a Class 1 safety system requires improvement and completion to include the out of scope work as defined in UN REG WEC 000475. However, subject to the resolution of the Technical Observations there is no reason, on the basis on the information sampled to date, to indicate the PMS will be unsuitable as a Class 1 safety protection system.

Due to the recent changes to the DAS platform and architecture, the DAS design is at an early stage in its lifecycle. The Safety Case for the use of the DAS requires improvement, and also to be completed to include the output from all stages of the design and implementation lifecycle. However, subject to the resolution of the technical observations there is no reason, on the basis on the information sampled to date, to indicate the DAS will be unsuitable as a Class 2 protection system.

The Safety Case for the use of the PLS/DDS requires improvement, and also to be completed to include the out of scope work. However, subject to the resolution of the technical observations there is no reason, on the basis on the information sampled to date, to indicate the PLS/DDS would be unsuitable as a Class 2/3 control system.

However, if all of the Technical Observations raised by the TSC are adequately addressed, along with issues arising from a thorough review of the design submission by Westinghouse, it is the view of the TSC that there have been no findings to preclude the UK AP1000 C&I systems important to safety presented from meeting the intent of appropriate guidance and standards including SAPs, TAGs and international Nuclear Sector Standards.

Annex 7

TSC Task Summary - Review of System Level Architecture [10]

Note this information has been imported from a TSC report (Ref. 83) and the formatting of the TSC report has been retained.

This Annex refers to the Pre-Construction Safety Report (PCSR) and European Design Control Document (DCD), which are references to the:

> AP1000 Pre-construction Safety Report, UKP-GW-GL-732 Revision 2, Westinghouse Electric Company LLC, December 2009, (Ref. 22); and
>
> AP1000 European Design Control Document, EPS-GW-GL-700 Revision 1, Westinghouse Electric Company LLC, December 2009, (Ref. 27);

respectively.

The versions of the BSCs referred to in this Annex are:

> PMS UKP-PMS-GLR-001 Rev 0 November 2010 (Ref. 49).
>
> CIM UKP-PMS-GLR-002 Rev 0 November 2010 (Ref 98).
>
> DAS UKP-DAS-GLR-001 Rev 0 November 2010 (Ref. 50).

[10] Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 7

Annex: Review of the System-Level Architecture

This Annex summarises the outcome of the Technical Support Contractor's (TSC) review of the System-Level Architecture **for the Westinghouse UK AP1000 reactor design.**

This review follows on from the review of architecture-related claims and argumentation carried out in a preliminary activity during Step 3. The aim of this review has been to gain confidence that Westinghouse has adequate evidence to support the claims and argumentation relating to the conformance of C&I architecture to appropriate guidance and standards, including relevant HSE / ND Safety Assessment Principles (SAPs), Technical Assessment Guides (TAGs) and International Nuclear Sector Standards.

The components of the C&I System–Level Architecture considered are:

- **Plant and Safety Monitoring System (PMS) including the Component Interface Module (CIM),**
- **The Diverse Actuation System (DAS),**
- **Plant Control System (PLS),**
- **Data Display and Processing System (DDS),**
- **The In-core Instrumentation System (IIS),**
- **The Special Monitoring System (SMS),**
- **Radiation Monitoring System (RMS),**
- Operations and Control Centres System (OCS),

The intention of this review **was to use a sampling approach to the review of evidence to consider the adequacy of the Safety Case to demonstrate that the overall S**ystem-Level Architecture**, as defined by Chapter 6.7 of the UK AP1000 Pre-Construction Safety Report (PCSR) and Chapter 7 of the European Design Control Document (EDCD), meets the requirements of appropriate guidance and standards identified by HSE/ND as being relevant to the S**ystem-Level Architecture.

The review was to report on the following aspects of the overall C&I architecture for safety capability:

- **Review the evidence identified by Westinghouse to confirm, or otherwise, that conformance with the eighteen key SAPs identified by the HSE / ND as being relevant to C&I architecture have been adequately demonstrated,**
    - **ECS.1, ECS.2, EDR.1, EDR.2, EDR.3, EDR.4, ERL.3, ESS.1, ESS.2, ESS.3, ESS.7, ESS.18, ESS.21, ESS.23, ESR.1, ESR.3, ESR.7 and ERC.2,**
- **Review and sentence the responses to Technical Queries (TQs) raised in the Step 3 S**ystem-Level Architecture review **that were not closed in Step 3,**
- **Report on the responses to the Observations made in the HSE / ND Step 2 and 3 reports,**

Annex 7

- Review a sample of the evidence identified by Westinghouse in relation to the claims and arguments against the relevant SAPs for inclusion in the SAPs, Safety Case Maps (SCM) and Claims Arguments and Evidence (CAE) trail report,

- Review a sample of the evidence identified by the RP, in support of claims and arguments relating to a satisfactory demonstration of conformance with the TAGs and IEC Standards clauses, as agreed with the HSE / ND, subject to time and resource constraints,
    - Five level 1 Nuclear Sector IEC Standards were considered as relevant (IEC61513, IEC60880, IEC 62340, IEC 61226 and IEC60987),
    - TAG 003, TAG 046 and TAG 051.

The initial sample of evidence documents reviewed by the TSC indicated that the Westinghouse PCSR and supporting documentation required improvements. The HSE/ND and TSC undertook considerable additional work to provide Westinghouse with feedback on the improvements required to provide suitable documents as the basis for an effective GDA review. These improvements were required to provide a clear CAE trail for the adequacy of the safety and safety related equipment.

In response to this feedback, Westinghouse revised its primary documentation set and provided documents more suitable for review purposes in the form of Basis of Safety Case (BSC) documents for the PMS, CIM and DAS. In addition, Westinghouse has agreed to provide a BSC for the Distributed Control and Information System (DCIS) that consists of the PLS and the DDS. The BSC for DCIS is scheduled to be available in early 2011 and therefore is outside the scope of this review.

As a result, the Step 4 System-Level Architecture review is based on the following specific areas:

- Review a sample of SCM submissions presented by Westinghouse to demonstrate conformance to HSE / ND SAPs; ESS.21 – Reliability and EDR.2 – Redundancy, Diversity and Segregation,

- Review and sentence Westinghouse responses to TQs; TQ-214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 264, 265, 266, 267, 268, 277, 313, 314, 315, 331, 493, 752, 1117 and 1125,

- Review of Observations identified in the HSE / ND Step 2 C&I Assessment Report, as applicable to C&I System-Level Architecture,

- Review of responses to technical observations from the TSC Step 3, System-Level Architecture report,

- Review of the Observations identified in the HSE / ND Step 3 C&I Assessment Report, as applicable to C&I architecture,

- Review of adequacy of the Basis of Safety Case documents for the DAS, PMS and CIM,

- Review of C&I submissions with respect to the C&I architecture requirements of relevant TAGs and IEC Nuclear Sector Standard clauses,

- Review of Westinghouse responses to Regulatory Observation RO-AP1000-082,

Annex 7

- Technical meetings with Westinghouse and HSE / ND to provide clarification of TQ subject matter.

The PMS is the primary protection system for the UK AP1000 which is distributed across four divisions and is based on ABB AC160 technology. The AC160 platform and PMS reviews are reported in the Platforms and Pre-Developed Equipment report and Systems Important to Safety report respectively. This System-Level Architecture report addresses the adequacy of the PMS in the context of the overall C&I architecture.

The CIM is considered part of the PMS, the PLS controls various safety components via the CIM under supervision of the PMS based on implementation of priority logic in the CIM. A Regulatory Observation (RO-AP1000-082) was raised requesting Westinghouse include analysis of the spurious operation for each of the essential safety functions of the PMS within the design base of the plant, if the unmitigated consequences of such an event could result in a significant radiological release. In response to the Regulatory Observation, Westinghouse proposed the use of the CIM to prevent or block the potential for PMS spurious actuations, particularly with respect to interlocking the PMS automatic actuation of the Automatic Depressurisation System (ADS) valves.

The DAS is a safety system that provides an alternative means of initiating reactor trip, actuating selected Engineered Safety Features (ESF) and monitoring plant information. During the course of the initial TSC review, the HSE / ND raised a Regulatory Observation with Westinghouse regarding the overly complex nature of the proposed DAS design and the lack of diversity from the proposed CIM implementation. In response Westinghouse now propose to replace the platform hardware for the DAS with their 7300 series which uses diverse technology from that proposed on the CIM. The Platforms and Pre-Developed Equipment report and Systems Important to Safety report on the DAS 7300 platform and DAS system respectively, whilst the Diversity of System Implementing Reactor Protection Functionality report addresses CIM/DAS diversity.

The PLS consists of closed loop controllers and the DDS/OCS interface and provides the functions required for normal operation from cold shutdown through full power. The PLS controllers are based on Emerson Ovation technology, the Ovation platform and PLS reviews are reported in the Platforms and Pre-Developed Equipment report and Systems Important to Safety report respectively.

As a result of the additional effort deployed to discuss the proposed C&I architecture with Westinghouse, as described above, the TSC has only completed an initial review of the Displays & Controls which has noted some areas for improvement regarding classification and adequacy.

Within each PMS division, there is a communication bus for data distribution within the division referred to as the AF100 bus. Although the AF100 bus is not used for reactor trip or ESF actuation, it is communicating Class 1 information to the operator in the main control room and therefore is required to be qualified accordingly. Within the PMS BSC, Westinghouse has agreed that the AF100 communication will be qualified to Class 1 performing Category A functions for the UK.

The HSE / ND Observations identified in the HSE / ND Step 2 and Step 3 C&I Assessment Reports have been considered during this Task. The Observations made in the HSE / ND reports that are relevant in the context of this Task are shown below in italics. In addition, a summary of the status to the observation is provided:

Annex 7

- *Clarification required for overall specification of the C&I architecture design including the interface requirements between different systems*; This observation has been resolved based on the RP identifying an overall C&I requirements specification (*AP1000 I&C System Requirements Specification* APP-GW-J1-010 Rev 1) that states the requirements for the different systems and any interface requirements between C&I systems. It was noted that the document does not state the Categorisation or Classification requirements for the C&I systems; however, this has been subsequently addressed in documentation received from the RP during Step 4.

- *Substantiate reliability claims for the C&I systems (PMS, DAS and PLS)*; This observation has been resolved based on the RP undertaking a reliability sensitivity study (*AP1000 PRA Control and Instrumentation Sensitivity Cases Quantification* APP-PRA-GSC-254 Rev 1).

- *Produce an analysis of the adequacy of safety groups (e.g. addressing coverage of Postulated Initiating Events (PIE), reliability, Common Cause Failure (CCF) and single failures etc.)*; Coverage of PIE are addressed by the HSE/ND. The requirement for the RP to produce a reliability analysis is resolved based on the RP undertaking a reliability sensitivity study (as above point). The requirement for the RP to produce an analysis of single failures is resolved based on the PMS and revised DAS architecture being tolerant to single failures (both C&I safety systems have redundant channels). The TSC report reviewing diversity aspects of the UK AP1000 (*Diversity of Systems Implementing Reactor Protection Functionality* 37194/65385R) covers the requirement for a CCF analysis to be produced for the PMS and revised DAS architecture.

- *Substantiation of the DAS FPGA design (including alignment with the HSE / ND special case procedure for complex hardware)*; This observation has been resolved based on the proposed DAS design implemented using the Westinghouse 7300 platform that no longer contains FPGAs or complex hardware.

- *Clarification of the interconnectivity of systems on and off site*; As discussed earlier, the AF100 communication bus is used for data distribution within PMS divisions and will be qualified accordingly, a High Speed Link (HSL) connects the PMS divisions. Further observations relating to the interconnectivity of C&I systems are covered in the technical observation; T17.TO2.02. The HSE / ND is addressing cyber security and interconnectivity of systems off site.

- *Clarification of segregation of C&I systems to ensure a lower class system cannot frustrate the correct operation of a higher class system*; This observation is covered in the Technical Observation; T17.TO2.02.

In addition to these Step 2 and Step 3 HSE / ND Observations, other TSC observations have been considered by raising Technical Queries with Westinghouse that have been addressed in Step 4. As identified below, Technical Queries and observations that have not been satisfactorily addressed have been merged into a single set of Technical Observations that address specific topics. A total of six technical observations have been raised, these observations have been designated as TO1 or TO2 by the TSC depending on their significance, of which TO1 is the higher. Two of these observations have been designated as TO1 and four observations have been designated as TO2.

<u>Technical Observations designated as TO1</u>

Annex 7

The two TO1 technical observations are:

T17.TO1.01; During the review of the overall C&I architecture, observations have been made that relate to the spurious operation of the PMS and the use of a blocker device to provide, under certain conditions, an inhibit signal to the CIMs. The designer or future operator/licensee is requested to:

a) Produce a Failure Modes and Effects Analysis (FMEA) for the blocker device as part of the final design submission for the device,

b) Produce detailed calculation figures for the reliability assessment of the blocker device, including a justification for the use of any common components within the blocker device that may result in CCF,

c) Produce a safety plan for the blocker device, identifying the PMS and CIM documentation that will be updated,

d) Identify the situations when the manual override of the blocker would be used and produce a demonstration that the use of the manual override could not interfere with the normal operation of the blocker,

e) Demonstrate that power supply fluctuations do not cause the ADS blocking device to behave in an unsafe manner,

f) Produce a rigorous assessment and justification that the use of the CIM is the best solution to interlock and prevent the PMS automatic actuation of the ADS valves.

T17.TO1.02; During the review of the overall C&I architecture, observations have been made that relate to the provision of displays and controls in the Main Control Room (MCR) and Remote Shutdown Room (RSR). There are no Class 1 displays and controls provided in the RSR. In their absence, the designer or future operator/licensee is requested to:

a) Demonstrate why it is not reasonably practicable to provide Class 1 displays and controls in the RSR, the demonstration should address the SAPs (SAP ESS.3 and ESS.8 para 343 etc.) in relation to the provision of Class 1 display and control facilities to allow the monitoring and initiation of Category A functions (such as reactor trip),

b) Demonstrate why it is acceptable for the proposed hard RSR control to be routed into and processed within the PMS (as defined in the *Protection and Safety Monitoring System Architecture Technical Report*, WCAP-16675 Rev 3), in divergence with the IEC standard requirements for systems of a lower class communicating into a higher class system.

c) Produce a demonstration that all failure modes and effects of all of the C&I equipment, associated with the operation of the PMS (i.e. including sensors, controllers and actuators), have been adequately addressed. Note that the FMEA for the PMS (WCAP-16438 Revision 2) does not incorporate a demonstration of all failure modes, including the magnitude of the effects for all C&I associated with the PMS have been adequately addressed. e.g. sensors, squib valve controllers and actuators.

<u>Technical Observations designated as TO2</u>

The four TO2 technical observations are:

Annex 7

T17.T02.01; During the review of the overall C&I architecture, observations have been made that relate to redundancy and allowance for unavailability of equipment. The designer or future operator/licensee is requested to:

a) Produce a demonstration of adequate redundancy in the RSR as required by SAPs (EDR.2 and ESS.23), to allow the removal of equipment from service for testing such that the RSR is available when required,

b) Identify the exact role of the second set of displays and manual controls located in the Security Station of the Auxiliary Building (as described in the DAS basis of Safety Case) and demonstrate the second set of displays and manual controls are adequate for the intended role.

T17.T02.02; During the review of the overall C&I architecture, observations have been made that relate to segregation of C&I systems and the potential for failure propagation. The designer or future operator/licensee is requested to:

a) Produce a substantiation for the physical separation methods employed for all Class 1 plant component interfaces (actuators and valves) that maintain the required isolation between C&I systems of different classes in accordance with IEC standards and SAP ESS.18,

b) Produce a substantiation that the calculated parameters generated in the PMS, communicated to the PLS and used by both the PMS and PLS for protection and control purposes (as defined in the *Protection and Safety Monitoring System Architecture Technical Report*, WCAP-16675 Rev 3), do not provide the potential for common failure of the PMS and PLS and the failure independence requirements of EDR.3 and ESS.18 are satisfied,

c) In accordance with the requirements of IEC 61513, produce a demonstration that the C&I architecture minimises the risk and consequence of failure propagation and the techniques used to achieve this. This should include a demonstration of any system monitoring by internal or external means (enabling early detection of corrupted data) and/or any defensive interfaces enabling the system and its subsystems to identify corrupted inputs and/or erroneous interactions,

d) Confirm the thermocouple signals to the Class 2 DAS are isolated from the Class 3 IIS to eliminate the effect of failure propagation as required by SAP ESS.18, (i.e. failure of the IIS leading to failure of the DAS),

e) Produce a demonstration that failure of the redundant power supply diode auctioneering (as defined in the *Protection and Safety Monitoring System Architecture Technical Report*, WCAP-16675 Rev 3), would not affect the other redundant power supply from operating normally and lead to loss of the safety function of the PMS. In addition, produce a demonstration that failure of a power supply is revealed in accordance with the requirements of SAP ESS.21,

f) The *Protection and Safety Monitoring System Architecture Technical Report*, WCAP-16675 Rev 3) refers to 'qualified isolation devices' that are used for analogue and digital I/O interfaces sending information from the PMS to the PLS. However, no further details or safety justification of these devices is provided. The designer or future operator / licensee to produce a safety justification for the qualified isolation devices used within the PMS.

T17.T02.03; During the review of the SCM for EDR.2, observations have been made that relate to the adequacy of the evidence presented in the SCM for EDR.2; the designer or future operator/licensee is

Annex 7

requested to modify the SCM to demonstrate SAP conformance by addressing the observations stated below:

a) Lack of revision status of the identified evidence on the SCM,

b) DAS PRA requires updating to reflect revised DAS architecture,

c) The SCM claims the PLS NSSS controllers are internally redundant; however, the identified evidence does not support this claim,

d) The SCM identifies the System Test Plan for the PMS (APP-PMS-T5-001) that is identified as evidence for the PLS,

e) Identify the standards and clauses to support the claim that appropriate standards are applied to the PMS, DAS and PLS,

f) To enable a full and complete review of the SCM, the designer or future operator/licensee is requested to make available all evidence identified on the SCM in support of a claim.

T17.T02.04; Observation relating to the adequacy of the evidence presented in the SCM for ESS.21; the designer or future operator/licensee is requested to modify the SCM to demonstrate SAP conformance by addressing the observations stated below:

a) Lack of revision status of the identified evidence on the SCM,

b) The SCM claims that fail-safe features are provided and identifies evidence for the PMS; however, there is no evidence cited for the application of a fail-safe approach for the CIM and DAS,

c) The SCM implies that as the DAS is a diverse system providing a backup to the PMS, a claim of fail-safe is conferred. However, it is unclear how the DAS, as a diverse back-up to the PMS, achieves the provision of fail-safe,

d) To enable a full and complete review of the SCM, the designer or future operator/licensee is requested to make available all evidence identified on the SCM in support of a claim.

In summary, unresolved technical queries and observations from Steps 2 and 3 have been merged with those arising from this Step 4 review into an integrated set of Technical Observations with the result that the System-Level Architecture review has six Technical Observations, two of which are of higher significance.

One higher significance technical observation raised by the TSC is for the designer or future operator/licensee to address the observations associated with RO-AP1000-082. The matters incorporated are; the designer or future operator/licensee is requested to include analysis of spurious operation for each of the ESF of the PMS and identify the proposed mechanisms to block any spurious operation of the PMS.

The second higher significance technical observation is concerned with the provision of controls and displays. The regulatory expectation is that Class 1 displays and controls are provided in the RSR and the designer or future operator/licensee is requested to produce a claim (supported by arguments and evidence) as to the equipment used to shut down the plant safely in the event that the MCR is not habitable, including a justification that the equipment class is suitable given that the functions performed are of Category A.

Annex 7

However, if all of the Technical Observations raised by the TSC are adequately addressed, along with issues arising from Westinghouse's own thorough review of the design submission, it is the view of the TSC that there have been no findings to preclude the UK AP1000 C&I architecture presented from meeting the intent of appropriate guidance and standards including SAPs, TAGs and international standards.

Annex 8

TSC Task Summary - Diversity of Systems Implementing Reactor Protection Functionality [11]

Note this information has been imported from a TSC report (Ref. 92) and the formatting of the TSC report has been retained.

This Annex refers to the Pre-Construction Safety Report (PCSR) and European Design Control Document (DCD), which are references to the:

> AP1000 Pre-construction Safety Report, UKP-GW-GL-732 Revision 2, Westinghouse Electric Company LLC, December 2009, (Ref. 22); and
>
> AP1000 European Design Control Document, EPS-GW-GL-700 Revision 1, Westinghouse Electric Company LLC, December 2009, (Ref. 27);

respectively.

The versions of the BSCs referred to in this Annex are:

> PMS UKP-PMS-GLR-001 Rev 0 November 2010 (Ref. 49).
>
> CIM UKP-PMS-GLR-002 Rev 0 November 2010 (Ref 98).
>
> DAS UKP-DAS-GLR-001 Rev 0 November 2010 (Ref. 50).

[11] Where the TSC TOs within this Annex relate to Assessment Findings as defined in the main body of this report then the actions are against a licensee only.

Annex 8

Annex: Task Summary: Diversity of Systems Implementing Reactor Protection Functionality

This Annex summarises a review of the diversity of the control and instrumentation (C&I) systems that contribute to Category A functions in the UK AP1000 reactor design. The review was undertaken in Step 4 of GDA by a Technical Support Contractor (TSC) in support of the HSE/ND. The claims and argumentation presented by Westinghouse (WEC) were reviewed in the preceding Step 3. The GDA Step 4 review addressed, on a sample basis, the adequacy of the evidence identified in support of the diversity case for those C&I systems implementing Category A functions. The diversity related guidance and standards considered are those identified by the HSE/ND and include Safety Assessment Principles (SAPs), Technical Assessment Guides (TAGs) and international nuclear standards.

The regulatory expectation is that equipment that could give rise to a Common Cause Failure (CCF) with unacceptable consequence would be demonstrated to be fit for purpose by the use of appropriate guidance such as that contained in IEC 62340, Nuclear Power Plants - Instrumentation and control systems important to safety - Requirements for coping with CCF and the common position of seven European nuclear regulators and authorised technical support organisations. Their common position is presented in the document "licensing of safety critical software for nuclear reactors". Consequently, it is expected that, for example:

- Between the different systems used there is diversity in the:
    - Technologies including the hardware, software and programming languages,
    - Development tools and processes,
- The development teams used for each system are different, and
- The verification, validation and test teams are independent of those involved in development.

The systems which implement Category A functions are as defined by Chapter 6.7 of the AP1000 Pre-Construction Safety Report (PCSR) for the UK and Chapter 7 of the European Design Control Document (DCD), namely:

- Protection and Monitoring System (PMS), incorporating the Component Interface Module (CIM), and
- Diverse Actuation System (DAS).

The PMS is the primary protection system for the UK AP1000 and is based on ABB AC160 technology, which is a software based system. The CIM is part of the PMS but enables a non safety system (the Distributed Control and Information System, DCIS) to control various safety components under the supervision of the PMS. The DAS provides a diverse means, to the PMS, of: initiating reactor trip; actuating selected Engineered Safety Features (ESFs); and monitoring plant information. Both the CIM and the DAS were proposed to be implemented using substantially the same technology, i.e. based on Field Programmable Gate Array (FPGA) technology. WEC has more recently proposed to implement the DAS on WEC's 7300 platform (which is analogue hardware). DCIS is used to control the plant during normal operating conditions. While DCIS does not implement category 'A' functions, this review

Annex 8

has considered, where it is important to overall plant safety and reliability, diversity between the PMS, DAS and DCIS. Such diversity provides a major contribution to protection from common mode failures and helps minimise the risk of losing plant control and protection at the same time.

A sampling approach was used to review the WEC identified evidence in the GDA Step 4 process. The initial sample of evidence reviewed by the TSC indicated that the Westinghouse PCSR and supporting documentation required improvements. The HSE/ND and TSC undertook considerable additional work to provide WEC with feedback on the improvements required to provide suitable documents as the basis for an effective GDA review. The improvements included to take into account the requirements of international standards and HSE / ND SAPs. They were also to present information in terms of Claims, Arguments and Evidence (CAE) that together demonstrate the adequacy of the safety and safety related equipment. This required supplementing existing documentation on equipment performance and functions with, for example, documentation detailing implementation technology, development and life-cycle processes, and how independence and diversity are to be achieved.

In response to the feedback, Westinghouse revised its primary documentation set and provided documents more suitable for review purposes. This included the creation of separate Basis of Safety Case (BSC) documents by WEC for the PMS, CIM and DAS. All three BSC documents discuss diversity.

Presented in this report is the work undertaken and resultant findings of the diversity review for the UK AP1000. This work included:

- Consideration of HSE / ND Step 2 and Step 3 Observations identified in the HSE / ND Step 2 and Step 3 C&I Assessment Reports.
- Consideration of TSC GDA Step 3 report technical observations.
- Review of WEC responses to HSE/ND technical queries including TQ274, 275, 276, 277, 278, 279, 280, 327, 328 and 1115. Each of the technical queries was generated to seek clarification on diversity observations.
- Review of WEC submissions in response to HSE/ND Regulatory Observations raised during GDA.
- Review of the WEC Safety Case Map (SCM) submission and the supporting CAE trail to confirm or otherwise conformance to HSE/ND Safety Assessment Principle (SAP) EDR.2 regarding diversity.
- Review of Basis of Safety Case documents for the DAS, PMS and CIM.
- Review of C&I submissions related to PMS, CIM, DAS and DCIS in the light of requirements that are relevant to diversity from international Nuclear Sector Standards IEC-61513-2001 and IEC-62340-2007.
- Technical meetings with WEC and HSE / ND to provide clarification of TQ subject matter.

As part of the above, various activities were undertaken that required WEC to explain why it was acceptable to have substantially similar (i.e. non diverse) equipment offered for the CIM and DAS. This

Annex 8

delayed progress with the original intent and scope of the review. As WEC responses were not considered to be adequate initially, HSE / ND raised Regulatory Observation RO-AP1000-081 (CIM-DAS diversity). It is only since October 2010 that WEC have presented CIM-DAS diversity CAE that was considered sufficient for review.

The WEC responses to Step 2 and 3 HSE / ND observations that related to diversity, along with other TSC observations, have been considered and where necessary progressed by raising technical queries with WEC in Step 4. The responses to the Step 4 technical queries and other observations were reviewed. Via this process, many technical queries and observations were satisfactorily resolved. Step 2, 3 and 4 technical queries and observations that have not been satisfactorily addressed have been merged into a single set of Technical Observations by the TSC. These have been given a Technical Observation (TO) identifier and designated as TO1 or TO2 depending on their significance, of which TO1 is the higher.

A total of 10 Technical Observations have been raised from the Step 4 review. Of these, one has been designated as TO1 and nine have been designated as TO2. The observations are as follows:

- T18.TO1.01: Regulatory Observation RO-AP1000-081 was raised during GDA to progress observations related to the adequacy of diversity between the CIM and the DAS including the processes used in their development and implementation. While some actions from this RO have been resolved, the WEC response does not directly address three specific actions. The designer or future operator / licensee is requested to produce documentation to capture claims, arguments and evidence to adequately address the remaining incomplete responses to the following RO actions within RO-AP1000-081 (see GDA Issue GI-AP1000-CI-03). These are:
    - To produce a clear demonstration of diversity of development processes for the CIM and DAS.
    - To clearly explain the use of independent verification and validation (V&V) teams for CIM and DAS and for any V&V activities yet to be completed, and demonstrate that independent V&V teams were actually used. The justification should cover platform and application levels as well as hardware and software (where used). Some claims and arguments have been made but they are incomplete and those regarding the hardware are not supported by evidence.
    - To demonstrate diversity between the tools used for the development of CIM and DAS.
- T18.TO2.06: Aspects of diversity between PMS (including the CIM), DAS and DCIS are discussed in the BSC documents and in other sampled evidence. However, the justifications reviewed are not linked to the potential for common cause failures, do not cover all combinations of systems and do not consider diversity in sufficient detail e.g. in all sub-systems and components within those systems. Thus, a comprehensive justification that the potential for common cause failure has been minimised is still needed. The designer or future operator / licensee is requested to:
    - Demonstrate that common cause failure of all combinations of the DAS, PMS (including the CIM) and DCIS due to common features has been rigorously analysed. This may involve showing conformance to a relevant common cause failure standard such as IEC 62340. For the analysis to be comprehensive it should include consideration of common

Annex 8

cause failure at system and platform level and all sub systems and components within each system.

- Justify the adequacy of diversity between all combinations of the PMS (including the CIM), DAS and DCIS. This may involve building on the diversity justifications in the BSCs and in the response to RO-AP1000-081. However, these should be refined in accordance with all the diversity observations in this public summary.

- T18.TO2.11: The GDA Step 4 review of diversity considered the adequacy of the CAE identified by the WEC Safety Case Map for SAP EDR.2 regarding diversity. The review found one of the two claims to be too brief to be understandable and there to be no document reference on one of the three items of evidence referenced on the SCM, meaning it was unclear what document it referred to. It was also unclear what standards were being claimed by the SCM or how they were determined to be the relevant standards. Of the other two references, one only refers to PMS and DAS diversity while the other cites almost no evidence to support the arguments presented. There is also limited coherence between the information presented in the Basis of Safety Case documents and that in the SCM. The designer or future operator / licensee is requested produce revised documentation to improve the clarity of claims, arguments and evidence supporting SAP conformance with EDR.2 regarding diversity, to:
  - Clarify the meaning of the claim 'diversity incorporated'.
  - Provide precise references to the evidence so that it can be identified and also ensure it has revision control.
  - Ensure the evidence cited covers diversity between all combinations of PMS (including CIM), DAS and DCIS.
  - Ensure the documents cited provide evidence which substantiates the claims and arguments they are claimed to support.
  - Clarify against which standards conformance is being claimed and present the basis on which these standards were identified.
  - Ensure that there is coherence between the claims, arguments and evidence regarding diversity in the SCM and those in the DAS and PMS BSCs.

- T18.TO2.12: During the review of the PMS and DAS, WEC provided a sensitivity analysis (AP1000 PRA Control and Instrumentation Sensitivity Cases Quantification, APP-PRA-GSC-254, Revision 1) to demonstrate the impact of less onerous reliability claims on overall plant risk. However, the PCSR and DCD, which are central documents in the traceability of safety claims, have not been revised to reference the sensitivity study. The designer or future operator / licensee is requested to produce an update to the PCSR and DCD to incorporate the sensitivity analysis results.

- T18.TO2.18: To enable diversity issues to be assessed, one observation within GDA technical query TQ-AP1000-1117 requested details of the non-Emerson equipment intended for use in the Turbine Control System. The response from WEC was generally informative. However, it is unclear regarding the use of AC160 equipment as part of the Turbine Control System. The

Annex 8

designer or future operator / licensee is requested to produce a clear statement as to whether the Turbine Control System does or does not use any AC160 equipment. If it does use AC160 equipment then the implications for the adequacy of diversity between the PMS (which includes AC160 modules) and PLS should be analysed and its adequacy justified.

- T18.T02.19: Regarding the adequacy of diversity between the DAS and PMS, the DAS BSC sets out how diversity is claimed to be achieved against five of the six areas of NUREG/CR 6303 (design diversity, equipment diversity, human diversity, signal diversity and software diversity). The sixth area, functional diversity, is discussed in terms of IEC 62340. However, the arguments presented are not clear or adequately justified. The designer or future operator / licensee is requested to produce a DAS – PMS diversity analysis that includes claims, arguments and evidence to:

    - Comprehensively and explicitly cover diversity between the DAS and PMS. Some arguments in the DAS BSC seem to only refer to diversity within aspects of the development of the DAS rather than between the DAS and PMS.

    - Justify that the diversity is adequate against appropriate standards and guidance. While examples of equipment diversity are provided, there is no discussion or evidence to indicate whether the equipment diversity is sufficient or even whether this has been considered. This might be shown, for example, by conducting an analysis of all components (e.g. FPGAs, ASICs, discrete components, etc) used in the DAS compared to those used in the PMS.

    - Clarify and justify the level of conformance with IEC 62340 being claimed. The standard is discussed but the level of conformance that is being claimed is unclear. In addition, the arguments presented are not currently adequate as a justification as they are generalised, high level statements that are unsupported by any evidence or any significant explanation. For example, from section 5.5.2 of the DAS BSC: "The major area of difference between the two standards is that IEC 62340 requires independent, functionally diverse I&C subsystems to achieve diversity goals." Such statements need to be justified by arguments and evidence describing how the major areas of difference between the two standards have been determined (e.g. by there being an analysis comparing the requirements of the two standards).

- T18.T02.20: During the GDA Step 4 review of the PMS BSC, the following observations were made related to the adequacy of the PMS and DCIS diversity justification. The arguments and information presented indicate that at a top level diversity exists between many aspects of the Common Q and Ovation platforms. However, the analysis is insufficiently detailed to provide assurance that there is adequate diversity and consequently potential areas of common mode failure are not identified. For example, key modules in the PMS and DCIS contain Intel processors. However, the Intel x86 processors used in the numerous DCIS I/O cards are not mentioned; only the Motorola processor used in the controller is identified. Intel processors are also used in the PMS Common Q flat panel display and the DCIS Ovation Dell workstations. While these are identified in the PMS BSC, any risk of a common cause failure is ignored on the basis that they are different processors. However, processor designers routinely use parts of the design of one processor in another meaning identical design errors can exist in different processors from the same origin. Should such an error exist then it is theoretically conceivable that, for example, it could cause both the PMS and DCIS to present

Annex 8

incorrect information to a plant operator. As such faults, if they exist, have the potential to affect both the plant operation and protection systems then it is important that they are considered. The designer or future operator / licensee is requested to produce:

  - An analysis of PMS and DCIS diversity that is demonstrably comprehensive i.e. includes all the sub systems and components within both these systems.

  - A submission (e.g. revised PMS BSC) that incorporates the results from the above analysis.

- T18.T02.21: The CIM BSC mentions CIM – DAS diversity. However, the discussion of diversity only references the safety case map for EDR.2. It does not present any additional information or capture any of the information produced as part of the response to RO-AP1000-081. The adequacy of the diversity discussion in the safety case map is captured in observation T18.T02.11. In addition, of the two references identified on the safety case map as related to the CIM, one does not mention the CIM. The designer or future operator / licensee is requested to revise the claims, arguments and evidence justifying the adequacy of the CIM – DAS diversity. This should include the relevant observations from and responses to RO-AP1000-081 and T18.T02.11, and thereby provide a single point of reference for the CIM-DAS diversity justification.
- T18.T02.24: Regarding the PMS and DCIS platforms, Section 5.1 of the PMS BSC states that they were designed by different companies (ABB and Emerson respectively) and therefore design diversity is assured by completely isolated diverse design teams. However, the TSC was informed by WEC previously that the initial design of Ovation (the DCIS platform) was founded in WEC. This is not mentioned or considered by the statement in the PMS BSC. The designer or future operator / licensee is requested to confirm and produce evidence that demonstrates the design teams for the PMS and Ovation platforms have been independent throughout their development. This should include the period when Ovation was being designed by WEC.
- T18.T02.25: The BSCs discuss diversity associated with the PMS, CIM, DAS and DCIS. However, none of the diversity justifications in the BSCs (or seen in other sampled evidence) cover support equipment modules and components. In addition, T18.T02.20 has found that the diversity justifications presented are insufficiently detailed. The designer or future operator / licensee is requested to produce a documented analysis to justify diversity between PMS (including the CIM), DAS and DCIS support equipment modules and components. This should include, for example, modems, transceivers and low voltage DC power supplies and similar equipment. The format of the diversity analysis in section 5.2 of the PMS BSC rev. 0 provides a possible format for such analysis.

In summary, this review has considered the adequacy of diversity between the I&C systems implementing reactor protection for the UK AP1000 reactor design. Adequacy has been judged against appropriate guidance, including relevant SAPs, TAGs and international standards. The TSC has concluded that the documentation provided by WEC presenting claims, arguments and evidence to demonstrate the adequacy of the diversity provisions requires improvement. The areas for improvement are captured in the observations outlined above. These observations are based on the submissions WEC defined as within the scope for GDA and the evidence sampling approach used by the TSC. Consequently, while they provide a broad and robust indication of the areas for improvement, they should not be regarded as exhaustive. However, if all of the technical observations raised by the

Annex 8

TSC are adequately addressed, along with issues arising from Westinghouse's own thorough review of the design submission, it is the view of the TSC that there have been no findings to preclude the UK AP1000 C&I architecture presented from meeting the intent of appropriate guidance and standards including SAPs, TAGs and international standards.