Westinghouse UK
AP1000® GENERIC DESIGN ASSESSMENT
Resolution Plan for GI-AP1000-C&I-03
Diversity of PLS, PMS (including CIM) and DAS

MAIN ASSESSMENT AREA	RELATED ASSESSMENT AREA(S)	RESOLUTION PLAN REVISION	GDA ISSUE REVISION
C&I	PSA	4	0

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 of ONR C&I Assessment Report,GDA-AR-11-006Revision 0).
ACTION: GI-AP1000-C&I-03.A1	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.
RELEVANT REFERENCE DOCUMENTATION RELATED TO GDA ISSUE	
GDA Open Issues Documents	GI-**AP1000**-C&I-03, Revision 0 Step 4 C&I Division 6 Assessment Report, GDA-AR-11-006, Revision 0
Technical Queries	TQ-**AP1000**-274 & TQ-**AP1000**-1115
Regulatory Observations	RO-**AP1000**-81
Other Documentation	UKP-PMS-GLR-001

Scope of work:
Detailed diversity analysis reports shall be prepared and issued to substantiate that the DAS has an adequate level of diversity from both the PLS/DDS and the PMS.

Deliverables/description of work:
This resolution plan will result in a detailed C&I Diversity Analysis which addresses both NUREG/CR 6303 and IEC 62340 diversity requirements as well as other guidance for ONR assessment. This analysis will be referenced in the DAS, PMS, DCIS BSC's. Specifically the issuance of the analysis will ensure related GDA open issues related to C&I diversity are resolved per ONR expectations. The analysiswill contain a discussion of the methods and analyses to be performed for the systematic review of both NUREG/CR 6303 and IEC 62340 diversity requirements as well as other guidance in relation to the DAS having an adequate level of diversity from both the PLS/DDS and the PMS (including CIM). In addition, substantiated evidence will be provided for diversity-related design features established for defence-in depth against common mode failures. In cases, where there is a conflict between the standards, the analysis will identify the preferred solution and provide the justification on why Westinghouse believes this solution meets ONR expectations and requirements. The diversity analysis will include the revised requirements related to the PMS Spurious Operation blocking function as discussed in GI-**AP1000**-CI-04. <u>Background on Diversity Standards</u> To protect against latent faults in C&I system that might result in common case failures (CCFs), regulators have developed a variety of standards and guidance to mitigate their effect. For the United States, the Nuclear Regulatory Commission (NRC) has developed

NUREG/CR 6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems”. For international work, the International Electrotechnical Commission (IEC) has developed IEC 62340, “Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)”

For the United Kingdom, IEC 62340, “Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)” identifies requirements to mitigate CCFs in digital C&I systems.

IEC 62340 Overview

The IEC standard states that functional diversity forms the only possibility to provide protection against a postulated latent functional fault in the requirements specification. Functional diversity ensures that safety requirements are met even if latent faults are realised due to errors in requirements specifications.

The IEC standard requires diverse C&I functions of category A to be assigned to independent C&I systems and implemented in a way such that, upon failure of a protection function in one system, the safety requirements of the plant are still met by the functions performed by the other independent C&I systems. The principle of independent C&I systems is used to limit the influence of CCF to one C&I system only. In other words, C&I systems perform their safety functions independently so a CCF failure in another C&I systems does not prevent the total C&I system from performing the functions as intended.

Independent C&I systems which perform category A functions are to be designed so the likelihood of triggering a coincident failure of these systems from the same input signal transient is reduced to a level that is not relevant during the intended plant life. As such, independent C&I systems are required to not use shared components or services if the postulated failure of these shared components or services can cause a coincident failure of the independent C&I systems. In addition, the use of similar hardware or software for C&I systems shall be analysed to demonstrate that the potential for CCF is negligible.

For software based C&I systems, the sensitivity to CCF shall be analysed by assessing the potential application and the signal trajectories for the individual software modules.

Independent C&I systems shall not perform identical application functions where possible. If the implementation of identical sub-functions cannot be avoided due to the plant design, these identical sub-functions shall be fed at least with input signals from separate sensors.

The IEC standard requires the design of C&I systems performing category A functions to protect against propagation of failure inside the C&I system. The implementation of these features requires that the application adheres to the following:

1. C&I systems shall be designed so that system operation cannot be jeopardised by central subsystems which may require communication to all redundancies of a C&I system performing a category A function.
2. Faulty data shall be excluded from further processing within the application software.

3. All functions provided by the system software for the transfer of messages shall be implemented in such a way that the correct execution of these software transfer functions cannot be disturbed.
4. Correctness of the received data shall be checked prior to further processing.
5. Physical separation of redundant sub-systems shall be designed according to IEC 60709.

The IEC 62340 standard identifies that exchanging input data between redundant units can introduce dependencies between channels. This interaction is required to be analysed regarding CCF possibilities. On-line validation of input data (e.g. voting logic, communication quality checks) should be used as a means to limit the propagation of faulty data. Those input signals which are already known to be faulty (e.g. range overflow) should be tagged and excluded from further processing.

To reduce the risk of disabling redundancies caused by maintenance and online testing activities, means should be provided to detect these faults (e.g. online monitoring) during maintenance and means to terminate maintenance activities in a controlled way leaving the system in an acceptable state. The IEC standard identifies that online monitoring is necessary to improve the availability of the systems important to safety. Although not directly relevant to CCF, the IEC standard invokes the following clauses per IEC 60880:

1. A pre-determined defined state shall be adopted when online monitoring detects a fault.
2. The state shall be chosen on ‘fail safe’ principles. Although this may often be designed to cause a safety actuation, it may also be designed to prevent a spurious actuation if it could lead to a design basis event (DBE).
3. Reduction of the possibility that system failure can be caused by accumulation of unidentified hardware faults.

For safety actuations that are prevented or automatically initiated in the event of a fault identified by online monitoring, alarms shall be provided to the main control room.

The IEC standard cites experience gained in operating analogue C&I systems in mild environments. Hardware modules with latent manufacturing defects which behave as expected during system commissioning may show an increased fault rate as components age. As such, failures of hardware components shall be analysed and logged so the maintenance staff will be warned in advance and will be able to take countermeasures to prevent the triggering of a CCF. Components of the applied C&I technology may show a decreasing fault rate early in their life. A “burn-in” process at the component or system level should be performed prior to safety relevant operation.

In addition to the above, the IEC standard identifies specific requirements to provide counter measures to CCFs:

1. C&I systems performing category A functions shall be designed so their operational behaviour is free of unintended consequences from specific calendar dates
2. To prevent unauthorised and manipulations of the C&I systems, the requirements given in IEC 60880 shall be applied.
3. Digital C&I systems performing category A functions should be designed according to IEC 61513. In addition, the requirements of IEC 60880 to reduce the possibility of

CCFs shall be as follows:

- Application software should be separated in such a way that the processing of plant process data is entirely performed by the application software.
- The operation of system software functions should not be influenced by any data which depends on the plant status.

4. The application software shall be designed to be tolerant of invalid input signals or spurious short-term input transients, such that safe action is ensured but spurious actuations are avoided.
5. Faulty input signals shall be identified by online monitoring. If faulty signals are identified and processed by comparison of redundant information, then the dependencies introduced between redundant sub-systems shall be analysed for CCF possibilities.
6. If a C&I system performs different functions and if one or more signals used by one function are invalid, all other functions with valid input signals shall not be affected.
7. The software shall be designed to take safe action even in response to multiple coincident failures or apparent failures of input signals. This safe action should avoid DBE caused by spurious actuations.
8. For C&I systems performing category A functions, simultaneous activities shall be restricted to a single redundancy to avoid a resulting failure of more than one of the redundant trains, channels or sub-systems.
9. The effects of maintenance activity during power operation shall be analysed to prevent other C&I systems, which perform category A functions and which are not subject to this maintenance activity, from failing.
10. In cases where a hardware component needs to be replaced by a substitute, it shall be ensured by adequate qualification of hardware and software features and by verification of compatibility between replaced and existing components that the reliability of the C&I safety systems is not reduced.
11. To limit the effect of a degradation of component robustness due to ageing the useful lifetime of the C&I components should be analysed.

NUREG/CR 6303 Overview

NUREG/CR 6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems” identifies methods of analysing computer-based nuclear reactor protection systems that discovers design vulnerabilities to digital C&I common-mode failure.

During the late 1960s in USNRC work on improving reactor instrumentation system reliability the following conclusions were reached (NUREG-0493):

1. Random independent component or subsystem failures are adequately mitigated by redundancy and should not be an important part of concerns over control/safety interdependence.
2. Given adequate redundancy, the remaining concern is some sort of non-random, multiple failure or common-mode failure.
3. Physical and electrical independence is the beginning, not the end, of common-mode failure concerns. Related and almost-coincident failures of supposedly separate systems can occur because of functional interactions, shared signals, common design errors, common environmental effects, and human actions.

NUREG/CR 6303 identifies that diversity cannot be considered in the absence of independence; diverse protection system elements that are not independent are assumed to fail simultaneously through interdependencies. Thus, diversity is not a substitute for, nor should it be proposed instead of the independence required by regulation and by standard. Rather, diversity should be seen as a necessary accessory to independence for increasing system robustness in the face of unidentified common-mode failure.

NUREG/CR 6303 assumes diversity can be separated into six attributes, listed in alphabetical order:

1. Design diversity.
2. Equipment diversity.
3. Functional diversity.
4. Human diversity.
5. Signal diversity.
6. Software diversity.

Design Diversity

Factors increasing diversity between two designs meeting the same requirements, excluding the effects of human diversity, in decreasing order of effect are:

- Different technologies (e.g., analogue versus digital).
- Different approaches within a technology (e.g., transformer-coupled AC instrumentation versus DC-coupled instrumentation).
- Different architecture (i.e., arrangement and connection of components).

Equipment Diversity

Factors increasing equipment diversity between two groups or items of equipment in decreasing order of effect are:

- Different manufacturers of fundamentally different designs.
- Same manufacturer of fundamentally different designs.
- Different manufacturers making the same design.
- Different versions of the same design.

The NUREG identifies in computer equipment there are additional details which help in judging whether computer equipment is sufficiently diverse:

- Different CPU architecture (e.g., Intel 80X86 architecture versus Motorola 68000).
- Different CPU chip versions (e.g., Intel 80386 versus Intel 80486).
- Different printed circuit board designs.
- Different bus structure (e.g., VME versus Multibus II).

The NUREG cites that different CPU architecture is a very powerful sort of diversity, since this forces different compilers, linkers, and other auxiliary programmes to be used.

Functional Diversity

Factors increasing functional diversity between two independent subsystems in decreasing order of effect are:

- Different underlying mechanism (e.g., gravity convection versus pumped flow, rod insertion versus boron poisoning).
- Different purpose or function (e.g., normal rod control versus reactor trip rod insertion), control logic, and actuation means.
- Different response time scale (e.g., a secondary system may react if accident conditions persist for a time).

Human Diversity

Factors increasing the human diversity of a design in decreasing order of effect are:

- Different design organisation (i.e., company).
- Different engineering management team within the same company.
- Different designers, engineers, or programmers.
- Different testers, installers, or certification personnel.

The NUREG identifies that management has the most significant effect on diversity because management controls the resources applied and the corporate culture under which designers, engineers, or programmers work. Poor resource allocation and a lack of “quality” commitment can render the effectiveness of using different personnel null. The relative importance of the human diversity attribute is the most difficult to assess of all the diversity attributes.

Signal Diversity

Factors increasing signal diversity between two signal sources in decreasing order of effect are:

- Different reactor or process parameters sensed by different physical effects (e.g., pressure or neutron flux).
- Different reactor or process parameters sensed by the same physical effect (e.g., pressure versus water level sensed by differential pressure sensors using the same sensor element).
- The same reactor or process parameter sensed by a different redundant set of similar sensors (e.g., a set of four redundant water level sensors backed up by an additional set of four redundant water level sensors driving a diverse design of protective equipment).

Software Diversity

Factors increasing diversity between software designs meeting the same requirements, excluding the effects of human diversity, in decreasing order of effect, are:

- Different algorithms, logic, and programme architecture.

- Different timing, order of execution.
- Different operating system.
- Different computer language.

The software must differ significantly in parameters, dynamics, and logic to be considered diverse, but only if the “operating system” is sufficiently simple that it can be considered to be a small set of demand driven subroutines. More complex operating systems introduce significant difficulties in analysis and may limit the independence that can be achieved, regardless of the quality of the safety software that uses the operating system.

The major point the NUREG identifies is that once an assessment of diversity attributes is made, the results can be combined to make an overall decision or to declare, for instance, that sufficient signal diversity exists. The diversity attributes that assume the greatest importance are dependent upon the situation.

Schedule/ programme milestones:

Periodic status meetings will be conducted between Westinghouse and ONR personnel to ensure that C&I GDA open issues are being resolved in timely and quality manner.

Schedule Overview

The C&I Diversity Analysis Reports will be developed, internally reviewed and transmitted to the ONR.

As part of the development of the reports the following subtasks will be undertaken:

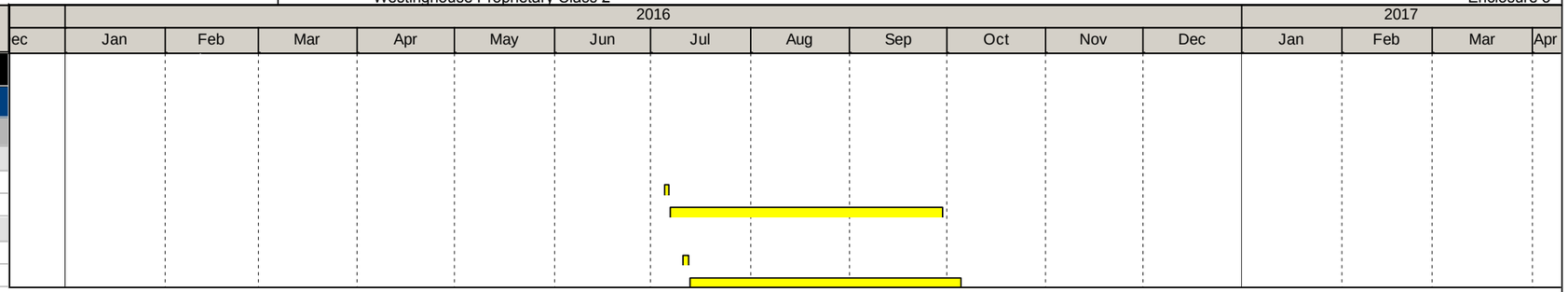
- Development of the report technical outlines.
- Review the specification and design of the DAS, PMS (including CIM) and DCIS (PLS/DDS).
- Identify what diversity analyses are to be undertaken (specs, tools, methods, algorithms, hardware and software etc.) and how the diversity analyses are to be completed (e.g. by review of detail design documentation) and confirming the criteria identified in IEC 62340 and NUREG 6303 as well as other guidance are suitable and sufficient when viewed against the full set of appropriate guidance (Safety Assessment Principles, IEC 61513, IEC 60880, and Common Position of Seven European Nuclear Regulators and Authorised Technical Support Organisations - 2010).
- Execute the Analysis
- Generate the Diversity Reports
- Perform appropriate technical and licensing reviews
- Respond to regulators comments
- If needed based on ONR comments, subsequent revisions of the reports will developed and issued.

Appropriate technical and licensing reviews will be conducted to ensure that the final version of the reports will demonstrate compliance to the appropriate SAP’s and

guidance provided by ONR.

Please see the following page for the schedule.

#	Activity Name
1	**UK Generic Design Assessment (GDA) Resolution Plans (51)**
2	**CONTROL & INSTRUMENTATION**
3	**CI.03 Diversity of PLS, PMS (including CIM) and DAS-Resolution Plan**
4	**CI.03 PMS DAS Diversity Analysis Revision 0**
5	PMS/DAS Diversity Analysis Rev.0-Submit to ONR
6	PMS/DAS Diversity Analysis Rev.0-ONR Review of Submittal
7	**CI.03 PLS DAS Diversity Analysis Rev. 0**
8	PLS/DAS Diversity Analysis Rev.0-Submit to ONR
9	PLS/DAS Diversity Analysis Rev.0-ONR Review of Submittal



Justification of adequacy:

The above formal methodology based on the Westinghouse QMS will address issues that ONR has raised in regards to the adequacy of the diversity of **AP1000**® C&I with respect to primary UK and US standards. This methodology will include appropriate technical and licensing reviews to ensure that the final version of the diversity analysis reports will demonstrate compliance to the appropriate IEC standards and guidance provided by ONR.

Westinghouse believes the aforementioned areas that will be addressed in the diversity analysis reports, in accordance to substantiation guidance contained in T/AST/051and per this Resolution Plan, will demonstrate that **AP1000** C&I diversity will be sufficiently robust to substantiate that the **AP1000** DAS has an adequate level of diversity from both the PMS and PLS/DDS to provide defence-in-depth against common mode failures.

Impact assessment:

The safety submission documents impacted by the implementation of the resolution plan are:

- UKP-DAS-GLR-001, "United Kingdom **AP1000** Basis for the Safety Case of the 7300 Based Diverse Actuation System."
- UKP-PMS-GLR-001, "United Kingdom **AP1000** Protection and Safety Monitoring System Safety Case Basis."
- UKP-GW-GLR-021, "United Kingdom **AP1000** Basis of Safety Case for the Ovation Based Distributed Control & Information System."
- UKP-GW-GL-793, Chapter 19, "**AP1000** Pre-Construction Safety Report."

Westinghouse expects that the PCSR chapter 19 will be updated to reinforce the diversity description as appropriate. Westinghouse also notes that other Chapters of the PCSR may require revision in addition to Chapter 19 as a result of the final version of the C&I Diversity Analysis Reports. If required, changes will be provided to other Chapters by the PCSR author.

Methodology:

Westinghouse and ONR personnel will conduct periodic review meetings during the course of the Resolution Plan execution to resolve in a timely manner any emergent issue that may impact Resolution Plan schedule and ensure ONR expectations are being met.

All Westinghouse system designs and associated documentation, like the C&I Diversity Analysis Reports, follow the Westinghouse Quality Management System (QMS) procedures as the methodology.

Specifically, quality and standardisation of technical documents generated as part of this

resolution plan are governed under the following procedures:

- Westinghouse QMS, “Westinghouse Electric Company Quality Management System”
  - Section 1.2, “Document and Data Control”
  - Section 2.1, “Quality Policy”
- Westinghouse Level II Procedure WEC 6.1, “Document Control”

Documents that are customer deliverables are subject to the Customer Satisfaction Process, discussed in Westinghouse Level II Procedure WEC 16.8, “Customer Satisfaction”

In addition, the following Westinghouse Level II Procedures provide important rules for creating and handling quality records, and electronic document management:

- WEC 17.1, “Records”
- WEC 17.2, “Electronic Approval”
- WEC 17.3, “Electronic Document Management”

The use of the Claims, Arguments and Evidence (CAE) structure for BSC documents as identified in T/AST/051, Issue 001, “Guidance on the Purpose, Scope and Content of Nuclear Safety Cases” will be employed in the C&I Diversity Analysis Reports.

Appropriate technical and licensing reviews will be conducted to ensure that the final version of the reports will demonstrate compliance to the appropriate SAP’s and guidance provided by ONR. Technical reviews are independent reviews that will focus on CAE being technically correct and producible; whereas, licensing reviews concentrate on ensuring regulatory requirements are properly addressed and substantiated.

Standards and practices, technology selection and justification, design tools and techniques, and verification and validation techniques will be identified and substantiated in the reports, as appropriate.

<u>Diversity Analysis Reports Development</u>

Detailed diversity analysis reports shall be prepared and issued that systematically review both NUREG/CR 6303 and IEC 62340 diversity requirements as well as other guidance in relation to the DAS having an adequate level of diversity from both the PLS/DDS and the PMS (including CIM). Claims and evidence for requirement compliance will be substantiated in the reports. There is not a one to one correspondence between IEC 62340 and NUREG/CR 6303. As such, Westinghouse will not assume that if the DAS diversity, as compared to PMS/CIM and PLS/DDS, meets the criteria of one of the standards, it also meets the other. Westinghouse will demonstrate compliance to both documents for DAS diversity separately, as compared to PMS/CIM and DCIS, since there is not a one to one correspondence between the two. In cases, where there is a conflict between the standards and Westinghouse designs, the analysis reports will identify the preferred solution and provide the justification of why Westinghouse believes this solution meets ONR expectations and requirements.

Particular attention will be paid to the following:

1. IEC 62340 is more prescriptive as compared to NUREG/CR 6303 to achieve the required level of diversity. The IEC standard requires specific design details to be implemented; whereas the NUREG defines areas of diversity attributes. The sum of these diversity attributes can be used to judge adequate diversity on a case by case basis.

2. IEC 62340 relies on functional diversity and system independence along with specific design features such as online monitoring to achieve diversity. NUREG/CR approaches diversity on a case to case basis where diversity attributes are weighed for the specific application.

3. The major area of difference between the two standards is that IEC 62340 requires independent, functionally diverse C&I subsystems to achieve diversity goals. NUREG/CR 6303 allows diversity goals to be met internally if the C&I system is properly designed and analysed.

In addition, the relevant TSC TOs identified in Step 4 of the C&I Division 6 Assessment Report, GDA-AR-11-006, Revision 0 will be evaluated early in the resolution plan execution cycle for inclusion in the issuance of the C&I Diversity Analysis Reports as appropriate.