New Reactors Programme

GDA close-out for the AP1000

GDA Issues GI-AP1000-CI-05 – Smart Device Justification

Assessment Report: ONR-NR-AR-16-032
Revision 0
March 2017

Published 03/17

For published documents, the electronic copy on the ONR website remains the most current publicly available version and copying or printing renders this document uncontrolled.

EXECUTIVE SUMMARY

Westinghouse Electric Company (Westinghouse) is the reactor design company for the **AP1000**® reactor. Westinghouse completed Generic Design Assessment (GDA) Step 4 in 2011 and paused the regulatory process. It achieved an Interim Design Acceptance Confirmation (IDAC) which had 51 GDA issues attached to it. These issues require resolution prior to award of a Design Acceptance Confirmation (DAC) and before any nuclear safety-related construction can begin on site. Westinghouse re-entered GDA in 2014 to close the 51 issues.

This report is the Office for Nuclear Regulation's (ONR's) assessment of the Westinghouse **AP1000** reactor design in the area of control and instrumentation (C&I). Specifically, this report addresses GDA Issue GI-AP1000-CI-05 for smart device justification.

This GDA issue arose in Step 4 due to the need to:

- develop a process for the safety justification of smart devices in the UK; and
- gain confidence in Westinghouse's ability to apply this process justifying three smart devices of different safety classes.

The Westinghouse GDA Issue Resolution Plan stated that its approach to closing the issue was to:

- produce the smart device justification process outlined in the form of a justification plan and a justification procedure;
- implement the process by justifying three smart devices selected as candidates for Class 1, Class 2 and Class 3 application.

My assessment conclusion is that:

- the justification process for smart devices proposed by Westinghouse in this GDA issue close-out is in line with the ONR's expectations for complex programmable devices (SAP ESS.27, Ref. 5; TAG 046, Ref. 6);
- Westinghouse's approach considers the relevant good practice in the UK for smart device justification (eg CINIF's Emphasis tool);
- with the justification examples, Westinghouse has demonstrated adequate capability to substantiate smart devices for nuclear safety applications in the UK; and
- the lessons learned from the examples were included in the justification plan and process documents.

My judgement is based upon the following factors:

- review of the submissions defining Westinghouse's approach to smart device justification;
- review of the three smart device justification examples (Class 1, Class 2 and Class 3 applications);
- inspections of the evidence associated with the justification examples; and
- Westinghouse's implementation of a design change proposal to address a weakness in the process of smart device identification.

The following matters remain, which are for a future licensee to consider and take forward in their site-specific safety submissions:

- to incorporate fully the design change proposal for smart device identification;
- to justify the adequacy of the process for the incorporation of the generic smart device justification in the overall C&I system safety case;

- to ensure that assessors assigned to the smart device justification have adequate specialist software and hardware competence; and
- to review submissions and implement the smart justification process for the substantiation of smart devices to be used in the UK **AP1000** design.

These matters do not undermine the generic safety submission and require licensee input / decision.

In summary, I am satisfied that GDA Issue GI-AP1000-CI-05 can be closed.

LIST OF ABBREVIATIONS

C&I	Control and Instrumentation
CINIF	C&I Nuclear Industry Forum
COTS	Commercial Off-The-Shelf
DAC	Design Acceptance Confirmation
GDA	Generic Design Assessment
ICBM	Independent Confidence Building Measures
IDAC	Interim Design Acceptance Confirmation
IEC	International Electrotechnical Commission
ONR	Office for Nuclear Regulation
PCSR	Pre-Construction Safety Report
PE	Production Excellence
RQ	Regulatory Query
SAPs	Safety Assessment Principles
TAG	Technical Assessment Guide
TO	Technical Observation
TSC	Technical Support Contractor

TABLE OF CONTENTS

Tables

Annexes

1 INTRODUCTION

1.1 Background

1. Westinghouse Electric Company (Westinghouse) completed GDA Step 4 in 2011 and paused the regulatory process. It achieved an Interim Design Acceptance Confirmation (IDAC) which had 51 Generic Design Assessment (GDA) issues attached to it. These issues require resolution prior to the award of a Design Acceptance Confirmation (DAC) and before any nuclear safety-related construction can begin on site. Westinghouse re-entered GDA in 2014 to close the 51 issues.

2. This report is the Office for Nuclear Regulation's (ONR's) assessment of the Westinghouse **AP1000** reactor design in the area of control and instrumentation (C&I). Specifically, this report addresses GDA Issue GI-AP1000-CI-05 for smart device justification.

3. The related GDA Step 4 report is published on the ONR website (Ref. 67), and this provides the assessment underpinning the GDA issue. Further information on the GDA process in general is also available on the ONR website (Ref. 68).

1.2 Overview of GI-AP1000-CI-05

4. This GDA issue was raised in Ref. 1 because the Requesting Party did not provide sufficient evidence in **AP1000** GDA Step 4 of an adequate approach to justify the use of smart devices in UK nuclear safety applications.

5. A smart device is generally a complex electronic component (either computer-based or programmed hardware). In most cases, smart devices are commercial off-the-shelf (COTS) components, not originally developed to nuclear standards. A more comprehensive definition of a smart device is provided in clause 5.2.2 of IEC 62671 (Ref. 14).

6. During Step 4, ONR highlighted that although, at a high level, Westinghouse's approach to smart devices was broadly acceptable, Westinghouse did not provide the detailed procedures supporting the substantiation process or the evidence of their capability to produce smart device justifications to meet expectations in the UK.

7. This GDA issue was therefore raised for Westinghouse to provide:

   - a detailed procedure for the justification of smart devices in the UK **AP1000** plant (Action 1 of GI-AP1000-CI-05); and
   - evidence of the implementation of this procedure for the justification of Class 1, Class 2 and Class 3 smart devices (Action 2 of GI-AP1000-CI-05).

1.3 Scope

8. The scope of this assessment is detailed in the assessment plan in Ref. 2.

9. The assessment carried out in the closure of this GDA issue focused on:

   - the adequacy of the process proposed by Westinghouse for the smart device justification; and
   - Westinghouse's capability to implement this process in the justification of real examples of smart devices in different safety classifications.

10. The scope of the assessment undertaken in the GI-AP1000-CI-05 close-out is appropriate for GDA because it enables a determination of whether the Requesting

Party has reached an adequate level of development of the justification process. It also ensures that it has suitable and sufficient competence and organisational capability to implement this process in realistic justification examples.

11. The scope is also in line with the expectations set for other Requesting Parties in GDA close-out (see Ref. 3).

1.4 Method

12. This assessment complies with ONR internal guidance on the mechanics of assessment within ONR (Ref. 4).

1.4.1 Sampling Strategy

13. It is rarely possible or necessary to assess a safety submission in its entirety, and therefore ONR adopts an assessment strategy of sampling.

14. In relation to the assessment of this GDA issue, a sampling approach was undertaken with regard to the evidence produced by Westinghouse to support the claims in the three justification reports produced for Action 2 of GI-AP1000-GI-05.

2 ASSESSMENT STRATEGY

2.1 Pre-Construction Safety Report (PCSR)

15. ONR's GDA Guidance to Requesting Parties (Ref. 70) states that the information required for GDA may be in the form of a PCSR. Technical Assessment Guide (TAG) no. 051 sets out the regulatory expectations for a PCSR (Ref. 69).

16. At the end of Step 4, ONR and the Environment Agency raised GDA Issue GI-AP1000-CC-02 (Ref. 71) requiring that Westinghouse submit a consolidated PCSR and associated references to provide the claims, arguments and evidence to substantiate the adequacy of the **AP1000** design reference point.

17. A separate regulatory assessment report (Ref. 72) is provided to consider the adequacy of the PCSR and closure of GDA Issue CC-02, and therefore this report does not discuss the C&I aspects of the PCSR. This assessment focuses on the supporting documents and evidence specific to GDA Issue GI-AP1000-CI-05.

2.2 Standards and Criteria

18. The standards and criteria adopted within this assessment are principally the Safety Assessment Principles (SAPs, Ref. 5), ONR internal TAGs, relevant national and international standards and relevant good practice informed from existing practices adopted on UK nuclear licensed sites.

2.2.1 Safety Assessment Principles

19. The key SAP applied within the close-out of this GDA issue is included within Table 1 below.

Table 1: List of key SAPs

SAP	Title	Reference in this report
ESS.27	Computer-based safety systems	Ref. 5

20. It should be noted that the assessment of the production excellence (PE) leg for smart device substantiation also considered other SAPs (eg EQUs, EMTs). However, the key features expected in the safety justification of smart devices are covered by ESS.27.

2.2.2 Technical Assessment Guides

21. The TAGs that have been applied as part of this assessment are set out in Table 2 below.

Table 2: List of key TAGs

Identification	Title	Reference in this report
TAG-046	Computer Based Safety Systems	Ref. 6
TAG-049	Licensee Core and Intelligent Customer Capabilities	Ref. 7
TAG-077	Supply Chain Management Arrangements for the Procurement of Nuclear Safety Related Items or	Ref. 8

	Services	

2.2.3 National and International Standards and Guidance

22. The national / international standards and guidance that have been used as part of this assessment are set out in Table 3 below.

Table 3: List of key national and international standards

Identification	Title	Reference in this report
CINIF Emphasis	Evaluation of Mission Imperative High-integrity Applications of Smart Instruments for Safety – tool and questionnaire version v2.4.1	Ref. 9
CINIF Cogs	D/632/4381/1 v1.0 Cogs8 Project Report: Part 1 – Smart instruments, Adelard LLP, 2011	Ref. 10
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems. International Electrotechnical Commission (IEC)	Refs 11–13
IEC 62671	Nuclear power plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality	Ref. 14
IEC 61513	Nuclear power plants – Instrumentation and control important to safety – General requirements for systems	Ref. 15
IEC 61226	Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions	Ref. 16
Seven Party Paper	Licensing of safety critical software for nuclear reactors. Common position of international nuclear regulators and authorised technical support organisations	Ref. 17

23. In the context of this GDA issue close-out, IEC 61513 (Ref. 15) and IEC 61226 (Ref. 16) were mainly used for general context (eg definitions, categorisation / classification).

24. The first two references in Table 3 were produced under the auspices of the C&I Nuclear Industrial Forum (CINIF), which comprises several UK nuclear stakeholders (including Licensees and Requesting Parties) and commissions C&I research activities of interest for application in nuclear installations in the UK. ONR is part of the forum as an observer.

2.3 Use of Technical Support Contractors (TSCs)

25. It is usual in GDA for ONR to use technical support, eg to provide additional capacity to optimise the assessment process, enable access to independent advice and experience, for analysis techniques and models, and to enable its inspectors to focus on regulatory decision-making and so on.

26. Table 4 sets out the broad areas of technical support that were utilised by ONR in GI-AP1000-CI-05 closure. This support was required to provide additional capacity and

to enable access to independent advice and experience. The TSC support enabled ONR to address the peak load of assessment required by the Westinghouse submission programme.

Table 4: Work packages undertaken by the TSC

TSC	Work package
Altran	Review of the main submissions against Action 1 (excluding the design change proposal in APP-GW-GEE-5328 and PCSR Chapter 5 in UKP-GW-GL-793)
Altran	Review of the main submissions against Action 2 (see Section 3 of this report for details)
Altran	Support in inspections of the evidence related to the justification examples submitted against Action 2

27. The TSC undertook the technical reviews under the close direction and supervision of ONR. The regulatory judgement on the adequacy or otherwise of the **AP1000** design was made exclusively by ONR. ONR raised all Regulatory Queries (RQs) and meeting actions with Westinghouse.

28. The TSC provided a report (Ref. 18) that addressed the scope of work listed above. The TSC also supported ONR in the review of responses to RQs and meeting actions placed on Westinghouse. The TSC report in Ref. 62 includes a summary statement of the results of its work and findings (ie Technical Observations (TOs)). I have reviewed the TSC's TOs and, as considered appropriate, taken them forward under Assessment Findings (see Annex 1). The TSC TOs provide further guidance on the GDA Assessment Findings and set expectations for their resolution. Within this report, references to the TSC TOs contained in Ref. 18 are provided using the unique TO identifiers (eg CI-05-TO2-nn).

2.4 Integration with Other Assessment Topics

29. GDA requires the submission of an adequate, coherent and holistic generic safety case. Regulatory assessment cannot therefore be carried out in isolation as there are often safety issues of a multi-topic or cross-cutting nature.

30. The following cross-cutting issues have been considered within this assessment:

- GI-AP1000-CC-02, in relation to the requirement in Chapter 5 of the PCSR for the identification and justification of smart devices; and
- GI-AP1000-EE-01, in relation to smart devices in electrical power supplies for the UK **AP1000** C&I systems.

2.5 Out-of-scope Items

31. The consideration of diversity requirements between smart devices was not resolved within this GDA issue closure and will need to be addressed as part of the justification of the overall C&I architecture in licensing space (see also AF-AP1000-CI-034; and Ref. 1 for context).

3 REQUESTING PARTY'S SAFETY CASE

32. As part of the close-out of Action 1 of this GDA issue (see Section 1.2 of this report and Ref. 1 for context), Westinghouse produced a smart device assessment process for the smart device justification to be applied to the UK **AP1000** design. The process consisted of:

- A justification plan for the smart devices (UKP-GW-GLR-017 Revs 1 to 4 respectively in Refs 29–32), which outlined the main steps in the justification, including:
    - the initial considerations to be made in the decision to use a smart device;
    - the relevant national / international standards to be considered;
    - a map presenting the relationships of the process for smart justification and other processes applicable in the safety case for the UK **AP1000** C&I systems;
    - the definition of roles and responsibilities;
    - the constitution of Westinghouse's smart device assessment team in charge of the smart justification; and
    - guidance on the expectations for competence and training of the individuals in the team.
- A smart devices justification process (UKP-GW-J0Y-004 in Revs A, 0, 1 and 2 in Refs 33–36), invoked by the justification plan in UKP-GW-GLR-017 (Revs 1 to 4 respectively in Refs 29–32), providing:
    - guidance on the expectations for the substantiation of PE and independent confidence-building measures (ICBMs) as defined in SAP ESS.27 (Ref. 5) and TAG-046 (Ref. 6);
    - guidance on the responses to the Emphasis questionnaire (Ref. 9);
    - guidance on the expectation for ICBMs for different safety classes; and
    - an intelligent customer approach for smart device justifications received from a third party.

33. It is noted that, while during Step 4 closure (see Ref. 1 for context) Westinghouse suggested three documents would be invoked by the justification plan (ie UKP-GW-GLR-017) to address the smart device justification at different safety classes (ie UKP-GW-J0Y-002, UKP-GW-J0Y-004 and UKP-GW-J0Y-005), the Resolution Plan for GI-AP1000-CI-05 (Ref. 20) clarified that the procedure for the smart justification for all safety classes would be included in the document identified as UKP-GW-J0Y-004.

34. In the close-out of this GDA issue, Westinghouse raised a design change proposal to address a gap in smart device identification (APP-GW-GEE-5328, Ref. 46). Westinghouse also highlighted that the licensing commitment for the safety justification of the smart devices for use in the UK **AP1000** C&I architecture was identified in the PCSR (Chapter 5 in UKP-GW-GL-793, Ref. 47).

35. The justifications produced against Action 2 of this GDA issue (see Section 1.2 of this report and Ref. 1 for context) provided evidence of the application of the process outlined in the resolution of GI-AP1000-CI-05 Action 1 to examples

(UKP-GW-GLR-028 (Ref. 58) for a Class 1 application; UKP-GW-GLR-034 (Ref. 59) for a Class 2 application; and UKP-GW-GLR-029 (Ref. 60) for a Class 3 application).

4 ONR ASSESSMENT OF GDA ISSUE GI-AP1000-CI-05

36. This assessment has been carried out in accordance with ONR document 'Purpose and Scope of Permissioning' (Ref. 19).

4.1 Scope of Assessment Undertaken

37. The focus of the assessment undertaken by ONR in GI-AP1000-CI-05 close-out is to determine the adequacy of Westinghouse's approach and capability to substantiate smart devices for their application in the UK **AP1000** plant.

38. The assessment covered all the submissions identified by Westinghouse in the GDA Issue Resolution Plan (Ref. 20) and described in Section 3 of this report.

4.2 Assessment

39. This section provides a summary of the assessment of the submissions provided by Westinghouse in the closure of GI-AP1000-CI-05. An in-depth review of Westinghouse's submissions against this GDA issue is captured in Ref. 62.

4.2.1 Action 1

40. In the early stage of this GDA issue close-out, I engaged in level 4 meetings with Westinghouse (Refs 21–22) to clarify the expectation in the UK for the justification of smart devices to be implemented in nuclear safety applications. ONR expectations regarding the safety substantiation of these types of complex programmable electronic devices are defined in SAP ESS.27 (Ref. 5) and TAG-046 (Ref. 6). As for computer-based systems, a two-legged safety substantiation is expected for smart devices. The production excellence (PE) leg in ESS.27 aims to demonstrate the robustness of the safety lifecycle utilised for the design and manufacture of the device. On the complementary leg, independent confidence building measures (ICBMs) are expected to provide an independent confirmation of the fitness for purpose of the device. The use of CINIF's Emphasis tool (Ref. 24) for the PE of smart device justification represents established relevant good practice in the UK.

41. Westinghouse proposed in Ref. 23 to use third-party assessment reports (eg IEC 61508 certification) for the justification of the PE leg of smart devices. I explained in Ref. 24 that for this to be adequate the following conditions need to be met:

- the certification is relevant to the specific product (eg same model/version and application type);
- all the evidence supporting the certification can be made available to the regulator by the third party;
- the role of intelligent customer is retained internally by the Requesting Party (licensee in licensing space); and
- the depth of the justification in the certification is commensurate with the substantiation expected in the UK (eg clause-by-clause compliance with the relevant standards).

42. ONR's expectation is that the use of an alternative approach has to be shown to be equivalent to the relevant good practice (set by Emphasis for smart devices for the PE substantiation) and any gap needs to be addressed and justified.

43. Westinghouse informed ONR in Refs 25–26 of its intention to revise its PE justification strategy, ie joining CINIF and approaching the substantiation of PE for smart devices thorough the use of the Emphasis tool.

Smart device justification plan (UKP-GW-GLR-017)

44. Westinghouse submitted Rev. 1 of UKP-GW-GLR-017 (Ref. 29). I found that Ref. 29 adequately clarified the context of the smart device justification, eg identifying the key steps in the smart device process and identifying considerations needed prior to starting a smart device assessment. The definition for a smart device in Ref. 29 was in line with the expectation in clause 5.2.2 of IEC 62671 (Ref. 14).

45. I raised a number of requests for clarification on Ref. 29 (RQ-AP1000-1348, Ref. 50; RQ-AP1000-1410, Ref. 51; RQ-AP1000-1519, Ref. 54; and RQ-AP1000-1593, Ref. 56), mainly regarding:

- the allocation of responsibilities in the smart device assessment between different departments in Westinghouse's organisation (eg engineering, procurement, Westinghouse's dedicated smart device assessment team);
- the approach to smart device identification (eg in packaged equipment); and
- the relationship between the justification plan and the justification process documents.

46. In RQ-AP1000-1593 (Ref. 56), I requested clarification from Westinghouse regarding the two-step approach it proposed for the smart device justification, ie providing a generic justification of the device without reference to a target application and then assessing the applicability of this generic justification for each specific application in the UK **AP1000** C&I architecture. In the response to the RQ (Ref. 56), Westinghouse explained that, while the former was addressed as part of the GI-AP1000-CI-05 close-out, the latter would be addressed in licensing when incorporating the smart device justification in the safety case for the relevant C&I systems. While addressing the RQ in Ref. 56, Westinghouse also:

- clarified, in Refs 36, 40, 42 and 45, the scope of the substantiation provided against this GDA (ie generic only) and the expectations before applying the justification for specific applications in the UK **AP1000** C&I architecture; and
- specified, in Refs 40, 42 and 45, the restriction of use in that a suitability assessment would be needed by competent personnel before the use of these generic justifications for any application in the UK **AP1000** plant.

47. I judged that this approach was broadly acceptable for this GDA issue closure because the smart justification process provided against GI-AP1000-CI-05 covers the key technical aspects required in the smart device justification (eg in addressing SAP ESS.27). I also found the regulatory approach taken in this matter proportionate in GDA because:

- the detailed arrangements for the incorporation of the smart device justification in a safety case need to be agreed with the future licensee; and
- a database of pre-qualified smart devices has been used elsewhere in the UK nuclear industry and the approach appears to be acceptable, provided that personnel with a strong competence in smart device substantiation can demonstrate the adequacy of the generic justification for the target application.

48. On this basis, I raised an assessment finding for the licensee to justify the adequacy of the arrangements in place for the verification of a generic smart device justification for a specific application in the UK **AP1000** C&I architecture (see Annex 1, point (a) of assessment finding CP-AF-AP1000-CI-003).

49. In the RQ full responses (Refs 50, 51, 54 and 56) and in further revisions of the documents (Refs 30 and 31), Westinghouse committed to:

- cover the intelligent customer approach to purchased justifications in UKP-GW-J0Y-004 (see the assessment of UKP-GW-J0Y-004 in Refs 33–36 later in this section of the report); and
- address the issue regarding the smart identification with a design change in APP-GW-GEE-5328 (Ref. 46, see the assessment of UKP-GW-J0Y-004 in Refs 33–36 later in this section of the report).

50. Rev. 4 of the justification plan (Ref. 32) clarified the remaining points in the outstanding RQs, eg describing how this justification plan document would fit in the context of other Westinghouse procedures and the reliability targets for various safety classes (ie Class 1/SIL 3–4: pfd 10^{-3}/10^{-4}; Class 2/SIL 2: pfd 10^{-2}; Class 3/SIL 1: pfd 10^{-1}).

51. I consider that Rev. 4 of the justification plan document is adequately developed to meet the expectations set for this GDA issue close-out.

Smart device justification process (UKP-GW-J0Y-004)

52. As clarified in UKP-GW-GLR-017 Rev. 4 (Ref. 32), the smart device assessment process in UKP-GW-J0Y-004 (Refs 33–36) is invoked when:

- a smart device has not been previously justified by Westinghouse; or
- a justification is available from a third party and its adequacy needs to be assessed internally as an intelligent customer; or
- a justification is contracted by Westinghouse to a third party.

53. Because of the justification examples provided by Westinghouse against Action 2 of GI-AP1000-CI-05 (ie Class 1 and 3 assessed internally by Westinghouse; Westinghouse's intelligent customer role on a purchased Class 2 justification), I assessed the first two options above as part of this GDA issue close-out. Westinghouse explained in Refs 29 and 50 that commissioning smart justifications to third parties could also be considered during licensing. Although a high-level approach to externally contracting justifications is outlined in UKP-GW-J0Y-004 (Refs 33–36), Westinghouse did not provide in GDA any example of the application of this process to ensure that its outcome was commensurate with an internal smart device justification (eg similar robustness of the justification and equivalent ownership of the results / assumptions of the justification). A detailed clarification of this was not expected in the close-out of this GDA issue, which focused on Westinghouse's internal capability to substantiate a smart device for a nuclear application in the UK. However, if this option is considered post-GDA closure, the licensee will need to clarify the arrangements in place to ensure that the same expectations set for internal justification are met when contracting out smart device justification activities (see Assessment Findings in Annex 1, in particular point b.).

54. Westinghouse submitted three revisions of the justification process (Rev. A in Ref. 33; Rev. 0 in Ref. 34; and Rev. 1 in Ref. 35). At high level, I found that the justification process document in Rev. 0 covered the fundamental expectations for the smart device justification (ie SAP ESS.27 in Ref. 5; and TAG-046 in Ref. 6) and showed a general understanding of the key standards and guidance to be considered in the justification (eg IEC 62671 in Ref. 14; IEC 61508 in Refs 11–13; and the Seven Party Paper in Ref. 17). Rev. 0 of UKP-GW-J0Y-004 (Ref. 34) considered key pieces of research activity carried out within the framework of UK CINIF research activities

(eg regarding the use of Emphasis as per Ref. 9 and on selection of ICBMs as per Ref. 27).

55. In the assessment of Refs 33–35, I raised two RQs (RQ-AP1000-1465, Ref. 52; and RQ-AP1000-1596, Ref. 57), requesting clarification regarding:

- Westinghouse's guidance to its assessors on the use of the Emphasis tool;
- Westinghouse's approach to the identification of compensating measures to address gaps in the PE leg;
- the justification of the adequacy of the set of selected ICBMs for different safety classes;
- training and competence requirements for the dedicated smart assessment team;
- Westinghouse's arrangements as intelligent customer when procuring third party's smart justifications; and
- the assumptions and boundaries of the generic smart device justifications.

56. In the assessment of Rev. 2 of UKP-GW-J0Y-004 (Ref. 36), I verified that these TOs were adequately addressed to meet ONR's expectations for GDA and that the document incorporated the key lessons learned from the three justification examples produced against Action 2 of GI-AP1000-CI-05 (see also RQs in Refs 53, 55, 58, 59, 60 and 61). On the basis of the review of Ref. 36, I found that the process developed by Westinghouse for smart device justification adequately addressed the expectation for the closure of Action 1 of this GDA issue. I raised an assessment finding (see Assessment Findings in Annex 1, in particular point f.) for the licensee to revise the document to address some outstanding points which I did not judge relevant for this GDA issue closure but which should be addressed in licensing/site-specific phases.

57. One of the key aspects that emerged in the close-out of this GDA issue action was the need for both software and hardware specialist competence to adequately produce (or evaluate as an intelligent customer) a safety justification for a smart device. Although the high-level requirements for assessors are set out in Ref. 37, it will be for a licensee to define an adequate process of assignment of personnel to the task, taking into consideration the safety class of the application and the complexity of the device (eg software, architecture and type). I raised an assessment finding (see Annex 1, point (c) of assessment finding CP-AF-AP1000-CI-003) for the licensee to clarify the detailed arrangements for this matter.

<u>Design change proposal on smart device identification (APP-GW-GEE-5328)</u>

58. The identification of the presence of smart devices represents a particularly important task, especially where packaged equipment is purchased and the vendor is not fully aware of the regulatory expectations for the justification of programmable devices. I requested clarification about Westinghouse's process for smart identification in RQ-AP1000-1348 (Ref. 50) and RQ-AP1000-1410 (Ref. 51).

59. Westinghouse acknowledged a potential gap in its non-Class 1E equipment procurement process, which relates to non-safety-related systems according to the US safety classification (see, eg, IEEE 603-2009). While in other regulatory contexts the safety demonstration is focused on the Class 1E equipment, in the UK there are systems implementing Cat B and C safety functions that fall into the non-Class 1E category. Westinghouse committed to address the potential gap with a design change, describing an integrated approach for smart identification across all technical disciplines.

60. Westinghouse submitted the design change proposal (APP-GW-GEE-5328 in Rev. 0, Ref. 46) and included this design change in Rev. 9 of the design reference point for the UK **AP1000** design (Ref. 48).

61. Westinghouse stated in Ref. 46 that, in the procurement process for the UK **AP1000** plant, it will require each vendor to provide a definitive statement either in the purchase order or in requirements traceability documentation as to whether or not complex programmable equipment is included.

62. The design change proposal in Ref. 46 also clarified that:

- A new design requirement for smart device identification and justification will be included in the UK **AP1000** programme in accordance with the requirement capture process outlined in Ref. 49. The requirement will point to the smart justification plan (UKP-GW-GLR-017 in Ref. 32), which invokes the process document (UKP-GW-J0Y-004 in Ref. 36) for smart device justification.

- Appropriate subject matter experts in smart device justification will be in charge of the activity across all the technical areas.

63. While Ref. 46 captured the changes needed in the standard **AP1000** top-tier design criteria documents, Westinghouse acknowledged in Ref. 46 that the full scope of the impacted documents will be identified during detailed design work when a full plant assessment is carried out. A 'known issue' was raised in Westinghouse's dedicated tool (KI-00000227 in Smart Plant® Foundation) to capture this open point.

64. Westinghouse explained in Ref. 46 that the optimal solution for implementing APP-GW-GEE-5328 (Ref. 46) will be defined in detail when the contractual arrangements with the licensee are set out.

65. I judge that this design change proposal in Ref. 46 is sufficiently developed for this GDA issue closure, as the Requesting Party has adequately addressed the ONR's concerns about smart device identification and requirement capture. I have raised an assessment finding for the licensee to demonstrate the adequacy of the detailed arrangements being carried forward, eg the form of the statement requested from the vendors for smart identification, the closure of the known issue KI-00000227 and other details of the implementation of APP-GW-GEE-5328 (Ref. 46, see Annex 1, point (d) of assessment finding CP-AF-AP1000-CI-003).

Chapter 5 of the **AP1000** PCSR

66. In Ref. 49, Westinghouse described the use of the PCSR as a means of capturing licensing commitments to inform the system requirements documents. As part of the resolution of GI-AP1000-CI-05 Action 1, Westinghouse confirmed its intention to include in the PCSR a licensing commitment dealing with the identification and justification of smart devices.

67. Westinghouse proposed to address the licensing commitment on smart devices in PCSR Chapter 5 (engineering principles) rather than in the dedicated C&I PCSR chapter (ie Chapter 19), because the presence of smart devices affects many disciplines (eg C&I, electrical, mechanical). I was content with this proposal, because it ensures cross-discipline alignment.

68. I have reviewed Section 5.12 of the PCSR Chapter 5 (Ref. 47) and confirmed that this section is in line with the design change proposal in Ref. 46. The reference in PCSR Chapter 5 to the smart device justification process and plan (UKP-GW-GLR-017 and UKP-GW-J0Y-004 in Refs 32 and 36) also provides sufficient confidence that the

approach taken for any smart device will be in line with the approach proposed against GI-AP1000-CI-05 Action 1 closure.

4.2.2 Action 2

69. Action 2 of GI-AP1000-CI-05 requires Westinghouse to apply the process defined in UKP-GW-GLR-017 and UKP-GW-J0Y-004 (respectively in Refs 32 and 36) to three justification examples, one per safety class (ie Class 1, Class 2 and Class 3).

70. As part of my assessment of these justification examples, I inspected the evidence associated with each safety justification. The approach I adopted in the inspection was to select a sample of key questions in the Emphasis tool (representing a number of essential requirements in IEC 61508, Refs 11–13) and to verify whether the evidence adequately supported the argument in the smart device justification. I also considered the safety substantiation using the CINIF Cogs approach (Ref. 10), ie selecting key goals in Cogs and verifying how they are covered by Westinghouse's responses in the Emphasis questionnaire and related evidence.

Class 1 smart device (UKP-GW-GLR-028)

71. Westinghouse submitted the justification report for an electrical circuit breaker proposed for a Class 1 application (UKP-GW-GLR-028, Rev. 0, Ref. 37). I assessed this submission and found that it fell short of ONR's expectations for the depth of the substantiation of the PE leg of SAP ESS.27 (RQ-AP1000-1518 in Ref. 53). The ONR expectation is that, as well as recording the answers to the Emphasis questionnaire, the justification report should record and explain the rationale behind these responses and point to the evidence supporting the argument.

72. In response to RQ-AP1000-1518 (Ref. 53), Westinghouse provided a revised version of the document (UKP-GW-GLR-028, Rev. 1, Ref. 39), explaining the engineering judgement that resulted in the answers to the Emphasis questionnaire.

73. I inspected the evidence associated with the safety substantiation. As a result of the assessment of Rev. 1 (Ref. 39) and the inspection (Ref. 63), I raised an RQ (RQ-AP1000-1628, Ref. 58); mainly about the justification of the adequacy of compensating measures proposed against gaps in the PE leg.

74. Westinghouse addressed the points raised in RQ-AP1000-1628 in UKP-GW-GLR-028 Rev. 2 (Ref. 40), identifying the outstanding modifications required to the document as open items for a future revision. ONR's expectation for Class 1 set for other GDA issue closures (see Ref. 3) is that, because of the proportionate effort expected for the higher safety class, a trial justification would be acceptable during GDA, provided that essential aspects of both legs of SAP ESS.27 are addressed and a clear definition of the outstanding activities necessary to complete the justification are identified. On this basis, I am satisfied that Ref. 40 adequately addressed the expectation for the Class 1 justification within GDA. I raised an assessment finding (see Annex 1, point (e) of assessment finding CP-AF-AP1000-CI-003.) requesting the licensee to address the open points in this document if this device was intended to be used in any safety application in the UK **AP1000** C&I architecture (ie Class 1 or lower).

75. In addition to the Class 1 smart device justification, Westinghouse also produced a smart device checklist (Ref. 38). The use of a smart device checklist was discussed during GDA Step 4 (Refs 1 and 66) as a way to demonstrate that the key aspects of the Seven Party Paper (Ref. 17) are covered in the smart device substantiation. After the submission of Ref. 38 for the Class 1 justification example, Westinghouse clarified in Ref. 55 that it did not intend to provide the same checklists for the Class 2 and Class 3 justification examples. The argument proposed was that, after development of the Westinghouse internal process for smart justification, the intent of the checklist was

covered in the internal smart device justification procedure (UKP-GW-GLR-017, Rev. 4 in Ref. 32; and UKP-GW-J0Y-004, Rev. 2 in Ref. 36). Given Westinghouse's explanation and consideration of the key aspects of the Seven Party Paper (Ref. 17) both in UKP-GW-J0Y-004 and in UKP-GW-GLR-017, I found that discontinuing the use of the smart device checklist for Class 2 and Class 3 to be acceptable in the context of this GDA issue closure.

Class 2 smart device (UKP-GW-GLR-034)

76. For the Class 2 justification example, Westinghouse proposed to purchase a justification from a third party and assess its adequacy internally. Considering that Westinghouse had already proposed to justify internally the smart devices for Class 1 and Class 3 applications, I found this approach broadly acceptable. However, I set the expectation that, as an intelligent customer, Westinghouse should achieve in the Class 2 example the same level of confidence provided by an internal justification. ONR's expectation regarding the intelligent customer approach is set out in TAG-49 (Ref. 7) and TAG-77 (Ref. 8).

77. Westinghouse submitted a justification for a variable speed drive smart device (UKP-GW-GLR-034, Rev. 0, Ref. 41), candidate for a Class 2 application. I assessed the submission in Ref. 41 and organised an inspection to sample the evidence associated with this justification. The outcome of the inspection is recorded in Ref. 64.

78. As a result of this assessment, I raised two RQs (RQ-AP1000-1645, Ref. 59; and RQ-AP1000-1690, Ref. 61). The main issue raised in these RQs was the approach to the third-party justification as an intelligent customer, which fell short in providing sufficient confidence in the suitability of the device for Class 2 application and showed a lack of ownership of the justification by the Requesting Party.

79. Westinghouse responded to the RQs (Refs 59 and 61) and resubmitted the document in its Rev. 1 (Ref. 42). Considering the modifications in Ref. 42, I found that this document showed an acceptable understanding of the expectation for a Class 2 justification in GDA. I raised an assessment finding (see Annex 1, point (f) of assessment finding CP-AF-AP1000-CI-003) requesting the licensee to revise the document addressing the open points identified in the safety plan section of Ref. 42 and considering additional guidance in Ref. 62.

Class 3 smart device (UKP-GW-GLR-029)

80. Westinghouse submitted a report for the justification of a guided-wave radar smart device proposed for a Class 3 safety application (UKP-GW-GLR-029, Rev. 0, Ref. 43).

81. Rev. 0 of UKP-GW-GLR-029 (Ref. 43) showed similarities to Rev. 0 of UKP-GW-GLR-028 (Ref. 37) Class 1 device in terms of the lack of depth in the substantiation of the answers in the Emphasis questionnaire. I raised this concern in RQ-AP1000-1554 (Ref. 55), which also requested additional clarifications (eg regarding the selection of ICBMs).

82. Westinghouse responded to RQ-AP1000-1554 (Ref. 55) and submitted a revised version of the report (UKP-GW-GLR-029, Rev. 1, Ref. 44). As for the Class 1 justification report, an inspection was organised to facilitate access to the evidence associated with the Class 3 justification. The outcome of the inspection was recorded in Ref. 64. RQ-AP1000-1687 (Ref. 60) was raised as a result of the assessment of UKP-GW-GLR-029 Rev.1 (Ref. 44) and the related inspection, requiring (among others) clarifications on restriction of use and on compensating measures to address gaps in the PE.

83. Westinghouse submitted Rev. 2 of UKP-GW-GLR-029 (Ref. 45), which I found acceptable to address the expectation in Action 2 of GI-AP1000-CI-05 regarding smart devices for Class 3 safety application. I raised an assessment finding (see Annex 1, point (f) of assessment finding CP-AF-AP1000-CI-003) requesting the licensee to revise the document addressing the open points identified in the safety plan section of Ref. 44 and considering additional guidance in Ref. 62.

4.3 Comparison with Standards, Guidance and Relevant Good Practice

84. My assessment of the latest revision of the submissions against GI-AP1000-CI-05 identified that Westinghouse's approach proposed for smart justification was in line with the regulatory expectation in the UK.

85. My judgement is based on:

- Westinghouse's use of the relevant nuclear standard in the UK (eg Seven Party Paper, Ref. 17; and IEC 62671, Ref. 14);
- considerations of the expectations in the UK for complex programmable electronic components (ie two-legged approach in SAP ESS.27, Ref. 5; and TAG-046, Ref. 6); and
- Westinghouse's use of the CINIF's Emphasis tool for smart device justification.

86. In assessing Westinghouse's submissions and coming to this judgement, I verified the consistency of the regulatory approach against other GDAs (eg UK EPR, see Ref. 3)

4.4 Assessment Findings

87. During my assessment of GI-AP1000-CI-05, an assessment finding was identified for a future licensee to take forward in their site-specific safety submissions. Details of these TOs are contained in Annex 1.

88. These matters do not undermine the generic safety submission and are primarily concerned with the provision of site-specific safety case evidence, which will usually become available as the project progresses through the detailed design, construction and commissioning stages.

5 CONCLUSIONS

89. This report presents the findings of the assessment of GDA Issue GI-AP1000-CI-05 relating to the **AP1000** GDA closure phase.

90. In conclusion, I am satisfied that the submissions addressed this GDA issue because:

- Westinghouse developed a process for justification of complex programmable smart devices which is in line with UK regulatory expectations given in ONR SAP ESS.27 (see Table 1); and
- Westinghouse demonstrated its capability to implement this process in real applications using the smart device justification examples.

91. In the close-out of this GDA issue, I raised an Assessment Finding to capture a number of technical issues which are expected to be addressed in licensing space, when the detailed arrangements for smart device justifications are put in place.

92. Overall, on the basis of my assessment, I am satisfied that GDA Issue GI-AP1000-CI-05 can be closed.

6 REFERENCES

1. ONR-GDA-AR-11-006, Rev. 0, Step 4 Control and Instrumentation Assessment of the Westinghouse **AP1000** Reactor, November 2011. www.onr.org.uk/new-reactors/reports/step-four/technical-assessment/ap1000-ci-onr-gda-ar-11-006-r-rev-0.pdf
2. ONR-GDA-AP-14-001, Rev. 0, **AP1000** GDA C&I Assessment Plan, April 2015, TRIM Ref. 2015/149263.
3. ONR-GDA-AR-11-022, Rev. 1, GDA Step 4 and Close-out for Control and Instrumentation Assessment of the EDF and AREVA UK EPR™ Reactor, March 2013. www.onr.org.uk/new-reactors/reports/step-four/close-out/gi-ukepr-ci-01-close-out.pdf
4. ONR Guidance on Mechanics of assessment, TRIM Ref. 2013/204124.
5. Safety Assessment Principles for Nuclear Facilities, ONR, November 2014. www.onr.org.uk/saps/saps2014.pdf
6. NS-TAST-GD-046, Revision 3, Computer Based Safety Systems, April 2013. www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-046.pdf
7. NS-TAST-GD-049, Revision 5, Licensee Core and Intelligent Customer Capabilities, April 2016. www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-049.pdf
8. NS-TAST-GD-077, Revision 3, Supply Chain Management Arrangements for the Procurement of Nuclear Safety Related Items or Services, February 2015. www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-077.pdf
9. Evaluation of Mission Imperative High-integrity Applications of Smart Instruments for Safety – tool and questionnaire version v2.4.1. Retrieved from CINIF.
10. D/632/4381/1 v1.0, Cogs8 Project Report: Part 1 – Smart instruments, Adelard LLP, 2011. Retrieved from CINIF.
11. IEC 61508-1:2010, Nuclear power plants – Functional safety of electrical/ electronic/programmable electronic safety-related systems – Part 1: General requirements. www.iec.ch/functionalsafety/standards/page2.htm
12. IEC 61508-2:2010, Nuclear power plants – Functional safety of electrical/ electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems. www.iec.ch/functionalsafety/standards/page2.htm
13. IEC 61508-3:2010, Nuclear power plants – Functional safety of electrical/ electronic/programmable electronic safety-related systems – Part 3: Software requirements. www.iec.ch/functionalsafety/standards/page2.htm
14. IEC 62671:2013, Nuclear power plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality.
15. IEC 61513:2013, Nuclear power plants – Instrumentation and control important to safety – General requirements for systems.
16. IEC 61226:2010, Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions.
17. Licensing of safety critical software for nuclear reactors. Common position of international nuclear regulators and authorised technical support organisations. Revised 2015. www.onr.org.uk/software.pdf
18. ONR/T2723: Support for **AP1000** C&I GDA Issues Resolution Work Package Description for SMART Device Justification For Use, Altran, S.P1641.27.4.TSC267.4, Issue 1 – TRIM Ref. 2017/7227.
19. NS-PER-GD-014, Revision 5, August 2015, 'Purpose and Scope of Permissioning'. www.onr.org.uk/operational/assessment/ns-per-gd-014.pdf

20. Westinghouse UK **AP1000**® GENERIC DESIGN ASSESSMENT Resolution Plan for GI-AP1000-C&I-5 Class 1 Displays and Controls, Rev. 4 (revised). http://www.onr.org.uk/new-reactors/reports/step-four/westinghouse-final-res-plans/resolution-plan-gi-ap1000-ci-05.pdf

21. ONR-GDA-CR-14-271, **AP1000** C&I GDA Issues Resolution Plan – Contact Record, level 4 C&I extended meeting, January 2015, TRIM Ref. 2015/25711.

22. GDA Issue Close-out phase – Control and Instrumentation Assessment of the Westinghouse **AP1000** Reactor Control and Instrumentation GDA Issues Closure Guidance Document, February 2015, TRIM Ref. 2015/84414.

23. Westinghouse, GI-AP1000-CI-05, Use and Role of Third Party Assessment Reports in Smart Device Justifications – Level 4 C&I meeting presentation, April 2015, TRIM Ref. 2015/134036.

24. ONR-GDA-CR-15-011, **AP1000** C&I GDA Issues Resolution – Contact Record, Leve 4 C&I progress meeting, April 2015, TRIM Ref. 2015/144865.

25. ONR-GDA-CR-15-055, **AP1000** C&I GDA Issues Resolution – Contact Record, Level 4 C&I progress meeting, May 2015, TRIM Ref. 2015/198231.

26. **AP1000** C&I, WEC-REG-0457N, Revised, Convergence on the remainder of the CI-05 Resolution Plan – Level 4 C&I meeting presentation, November 2015, TRIM Ref. 2015/424883.

27. D/752/45008/1, v1.0, 'Guide to software analysis techniques', Adelard LLP, 2014. Retrieved from CINIF.

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

29. Westinghouse **AP1000** SMART Device Justification Plan, UKP-GW-GLR-017, Rev. 1, TRIM Ref. 2015/72116.

30. Westinghouse United Kingdom **AP1000** SMART Device Justification Plan, UKP-GW-GLR-017, Rev. 2, TRIM Ref. 2015/299113.

31. Westinghouse United Kingdom **AP1000** SMART Device Justification Plan, UKP-GW-GLR-017, Rev. 3, TRIM Ref. 2016/304638.

32. Westinghouse United Kingdom **AP1000** SMART Device Justification Plan, UKP-GW-GLR-017, Rev. 4, TRIM Ref. 2016/497331.

33. Westinghouse United Kingdom **AP1000** SMART Device Justification Process, UKP-GW-J0Y-004, Rev. A, TRIM Ref. 2015/367271.

34. Westinghouse United Kingdom **AP1000** SMART Device Justification Process, UKP-GW-J0Y-004, Rev. 0, TRIM Ref. 2016/148522.

35. Westinghouse United Kingdom **AP1000** SMART Device Justification Process, UKP-GW-J0Y-004, Rev. 1, TRIM Ref. 2016/449502.

36. Westinghouse United Kingdom **AP1000** SMART Device Justification Process, UKP-GW-J0Y-004, Rev. 2, TRIM Ref. 2016/497351.

37. Westinghouse United Kingdom **AP1000** SMART Device Assessment Summary Report for Substantiation of the Trip Unit for Use in Class 1 Safety Applications, UKP-GW-GLR-028, Rev. 0, TRIM Ref. 2016/53442.

38. Westinghouse United Kingdom **AP1000** SMART Checklist for the Class 1 Device, NNP-JNE-000656, February 2016, TRIM Ref. 2016/53450.

39. Westinghouse United Kingdom **AP1000** SMART Device Assessment Summary Report for Substantiation of the Trip Unit for Use in Class 1 Safety Applications, UKP-GW-GLR-028, Rev. 1, TRIM Ref. 2016/229957.

40. Westinghouse United Kingdom **AP1000** SMART Device Assessment Summary Report for Substantiation of the Trip Unit for Use in Class 1 Safety Applications, UKP-GW-GLR-028, Rev. 2, TRIM Ref. 2016/449509.

41. Westinghouse United Kingdom **AP1000** SMART Device Assessment Report for Siemens G120 Variable Speed Drive for Class 2 Applications, UKP-GW-GLR-034, Rev. 0, TRIM Ref. 2016/236386.

42. Westinghouse United Kingdom **AP1000** SMART Device Assessment Report for Siemens G120 Variable Speed Drive for Class 2 Applications, UKP-GW-GLR-034, Rev. 1, TRIM Ref. 2016/449518.

43. Westinghouse United Kingdom **AP1000** SMART Device Assessment Summary Report for Substantiation of the Magnetrol ECLIPSE 706 Guided Wave Radar Level Transmitter for Use in Class 3 Safety Applications, UKP-GW-GLR-029, Rev. 0, TRIM Ref. 2016/98961.

44. Westinghouse United Kingdom **AP1000** SMART Device Assessment Summary Report for Substantiation of the Magnetrol ECLIPSE 706 Guided Wave Radar Level Transmitter for Use in Class 3 Safety Applications, UKP-GW-GLR-029, Rev. 1, TRIM Ref. 2016/289050.

45. Westinghouse United Kingdom **AP1000** SMART Device Assessment Summary Report for Substantiation of the Magnetrol ECLIPSE 706 Guided Wave Radar Level Transmitter for Use in Class 3 Safety Applications, UKP-GW-GLR-029, Rev. 2, TRIM Ref. 2016/449534.

46. Westinghouse United Kingdom **AP1000,** APP-GW-GEE-5328, Revision 0 – Addition of Smart Device Identification and Justification Requirement for UK **AP1000**, October 2016, TRIM Ref. 2016/482388.

47. WEC-REG-1552N, Enclosure 1, UKP-GW-GL-793, Revision 1 – **AP1000** Pre-Construction Safety Report, 31 January 2017, TRIM Ref. 2017/43700.

48. Westinghouse United Kingdom **AP1000**, UKP-GW-GL-060, Revision 9 – **AP1000** Design Reference Point for UK GDA, November 2016, TRIM Ref. 2016/446340.

49. Westinghouse United Kingdom **AP1000**, UKP-GW-GLR-116, Revision 0 – UK **AP1000** Design C&I Requirements Management Overview, November 2016, TRIM Ref. 2016/449029.

50. RQ-AP1000-1348, Comments on SMART Justification Plan (UKP-GW-GLR-017, Rev. 1), August 2015, Full Response, TRIM Ref. 2015/299104.

51. RQ-AP1000-1410, Comments on SMART Justification Plan (UKP-GW-GLR-017, Rev. 2), November 2015, Full Response, TRIM Ref. 2016/167492.

52. RQ-AP1000-1465, Comments on UKP-GW-J0Y-004 Revision A – **AP1000** Smart Device Assessment Process, April 2016, Full Response, TRIM Ref. 2016/148514.

53. RQ-AP1000-1518, Comments on Smart Device Assessment Summary Report for Substantiation of the Trip Unit for Use in Class 1 Safety Applications (UKP-GW-GLR-028, Rev. 0), April 2016, Full Response, TRIM Ref. 2016/186226.

54. RQ-AP1000-1519, Comments on the full response to RQ-AP1000-1410 ('**AP1000** SMART Device Justification Plan', UKP-GW-GLR-017, Rev. 3 – Draft), April 2016, Full Response, TRIM Ref. 2016/167492.

55. RQ-AP1000-1554, Comments on UKP-GW-GLR-029 Revision 0 – SMART Device Safety Class 3 Justification Report, June 2016, Full Response, TRIM Ref. 2016/259987.

56. RQ-AP1000-1593, Outstanding Open Issues on GI-AP1000-CI-05, June 2016, Full Response, TRIM Ref. 2016/260218.

57. RQ-AP1000-1596, Comments on UKP-GW-J0Y-004 Revision 0 – Smart Device Justification Process, July 2016, TRIM Ref. 2016/276405.

58. RQ-AP1000-1628, Comments on UKP-GW-GLR-028 Revision 1 – SMART Device Assessment Summary Report for Substantiation of the Trip Unit for Use in Class 1 Safety Applications, August 2016, Full Response, TRIM Ref. 2016/331892.

59. RQ-AP1000-1645, Comments on UKP-GW-GLR-034 Revision 0 – SMART Device Assessment Report for Siemens G120 Variable Speed Drive for Class 2 Applications, October 2016, Full Response, TRIM Ref. 2016/398898.

60. RQ-AP1000-1687, Comments on UKP-GW-GLR-029 Revision 1 – Smart Device Assessment Summary Report for Substantiation of the Magnetrol ECLIPSE 706 Guided Wave Radar Level Transmitter, October 2016, Full Response, TRIM Ref. 2016/393751.

61. RQ-AP1000-1690, Comments Arising from the Class 2 SMART Device Inspection, October 2016, Full Response, TRIM Ref. 2016/398903.

62. ONR/T2723: Support for **AP1000** C&I GDA Issues resolution SMART Device Justification For Use, Altran, S.P1641.40.TSC267.4, Issue 2, March 2017, TRIM Ref. 2017/80924.

63. ONR/T2723: Support for **AP1000** C&I GDA Issues resolution Class 1 SMART Device Inspection, Altran, S.P1641.40.TSC267.4.1, Issue 1, July 2016, TRIM Ref. 2017/7255.

64. ONR/T2723: Support for **AP1000** C&I GDA Issues resolution Class 2 and 3 SMART Device Inspection, Altran, S.P1641.40.TSC267.4.2, Issue 1, September 2016, TRIM Ref. 2017/7253.

65. ONR Inspection Rating Guide, April 2016. www.onr.org.uk/intervention-records/onr-inspection-rating-guide.pdf

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

67. UK **AP1000,** GDA Step 4 report and publications, ONR. www.onr.org.uk/new-reactors/ap1000/reports.htm

68. Generic Design Assessment (GDA) of new nuclear power stations, ONR. www.onr.org.uk/new-reactors/index.htm

69. NS-TAST-GD-051 Revision 4 – The purpose, scope and content of safety cases. www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-051.pdf

70. ONR-GDA-GD-001 Revision 3 – New nuclear reactors: Generic Design Assessment Guidance to Requesting Parties. www.onr.org.uk/new-reactors/ngn03.pdf

71. Westinghouse UK **AP1000** Generic Design Assessment Resolution Plan for GI-AP1000-CC-02 PCSR, Rev. 3. www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-cc-02.pdf

72. ONR-NR-AR-16-038 – **AP1000** Assessment Report, GI-AP1000-CC-02, TRIM Ref. 2016/274964.

Annex 1

Assessment findings to be addressed during the Forward Programme – GI-AP1000-CI-05

Assessment finding number	Assessment finding	Report section reference
CP-AF-AP1000-CI-003	The Licensee shall: a. implement adequate arrangements to verify the suitability of generic smart device justifications (produced in accordance with UKP-GW-GLR-017 Rev. 4 and UKP-GW-J0Y-004 Rev. 2) for specific applications in the UK **AP1000** design; b. where the smart device justification is undertaken by a third party, ensure that the contract specification, the surveillance of external activities and the intelligent customer arrangements satisfy the process described in UKP-GW-J0Y-004 Rev. 2; c. ensure that the detailed arrangements for the selection and evaluation of the assessors performing smart device assessments take into account the specialist software and hardware competence required for justification of smart devices (eg commensurate with the safety class for the proposed application, the type and the complexity of the device); d. fully implement APP-GW-GEE-5328 Rev. 0 on the UK **AP1000** design and justify the adequacy of the detailed arrangements in place for smart device identification; e. complete the justification trial in UKP-GW-GLR-028 Rev. 2, should the smart device be considered for any safety application (Class 1 or lower) in the UK **AP1000** design; and f. review the GI-AP1000-CI-05 submissions and implement the smart justification process defined in UKP-GW-GLR-017 Rev. 4 and UKP-GW-J0Y-004 Rev. 2 for the substantiation of smart devices to be used in the UK **AP1000** design. For context, see Section 4.2 in this report and for further guidance on this assessment finding see Technical Observations CI-05-TO2-2.1.2.2-1, CI-05-TO2-2.1.2.2-2, CI-05-TO2-2.1.2.2-3, CI-05-TO2-2.1.2.2-4, CI-05-TO2-2.1.2.2-7, CI-05-TO2-2.1.2.2-8,	Section 4.2.1 and 4.2.2

	CI-05-TO2-2.2.2.1-4, CI-05-TO2-2.2.2.1-5, CI-05-TO2-2.2.2.1-8, CI-05-TO2-2.2.2.1-9, CI-05-TO2-2.2.2.1-11, CI-05-TO2-2.2.2.1-12, CI-05-TO2-2.2.2.1-13, CI-05-TO2-2.2.2.1-15, CI-05-TO2-2.2.2.1-16, CI-05-TO2-2.2.2.1-17, CI-05-TO2-2.2.2.3-3, CI-05-TO2-2.2.2.3-5, CI-05-TO2-2.2.2.3-6, CI-05-TO2-2.2.2.3-8 and CI-05-TO2-2.2.2.3-17 in Ref. 62.	