New Reactors Programme

GDA close-out for the AP1000 reactor

GDA Issue GI-AP1000-FS-08: Fault Schedule for AP1000

Assessment Report: ONR-NR-AR-16-028
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 LLC (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 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 GDA Issues.

This report is the Office for Nuclear Regulation's (ONR's) assessment of the Westinghouse **AP1000** reactor design in the area of fault studies. Specifically, this report addresses GDA Issue GI-AP1000-FS-08 "Fault Schedule for **AP1000**".

The provision of a tabular summary of the key aspects of a nuclear facility's safety case, commonly referred to as a 'fault schedule', is considered relevant good practice in the UK. The **AP1000** design, together with supporting documentation, was developed in the US where fault schedules are not routinely produced. As part of its interactions with ONR before the GDA pause, Westinghouse started to develop a fault schedule for the **AP1000** reactor; however, it did not provide a mature submission in time for assessment during Step 4.

In response to this GDA Issue, Westinghouse has:

- submitted preliminary versions of a revised fault schedule for discussion with ONR;
- subsequently updated the fault schedule to address feedback from discussions with ONR, changes to the safety case introduced by addressing the other 50 GDA Issues, and the application of its own internally quality assurance processes;
- submitted a final version of the revised fault schedule as an integral part of its Pre-Construction Safety Report (PCSR); and
- identified hazard schedules included with the internal hazards portion of the PCSR as a source of complementary information to the main fault schedule.

My assessment conclusions are:

- Westinghouse has produced a fault schedule with a format and scope that is both appropriate for its technology / safety case and is consistent with relevant good practice.
- Based on an extensive sample of reactor faults, the fault schedule is an adequate summary of the design basis safety case set out in the fault studies chapter of the PCSR and it also provides a useful 'starting point' for understanding the beyond design basis safety case described in the Probabilistic Safety Assessment (PSA) chapter of the PCSR.
- The fault schedule, complemented by hazard schedules, provides appropriate visibility to the graded approach applied in the **AP1000** safety case for Structures, Systems and Components (SSCs) that protect against internal and external hazards.
- The fault schedule and hazard schedules make a useful contribution to the PCSR, showing some of the expectations and properties set out in ONR guidance for what constitutes an adequate safety case.

I reached these judgements following an extensive sample of the fault schedule entries for reactor faults and internal / external hazards, and making comparisons against ONR's expectations set out in the Safety Assessment Principles (SAPs). Consideration was given to the scope, format, accuracy and completeness of the fault schedule.

It is important to note that an assessment of the adequacy of the underpinning safety case the fault schedule summarises was beyond the scope of this assessment report. Also, this

assessment has not attempted to verify the accuracy of every entry in the fault schedule; that is a matter for Westinghouse in accordance with its own internal quality assurance processes.

I found some weaknesses in the fault schedule's treatment of non-reactor faults. However, many aspects of the safety case in these areas were excluded from the scope of GDA Step 4 assessments (across various topic areas) and therefore I have judged it to be inappropriate to use the observed shortfalls as reasons to not close this GDA Issue. There is a clear expectation that areas of the safety case declared out of scope of GDA will need to be addressed during site licensing, and the fault schedule (as a 'live' aspect of the PCSR) will need to be updated to reflect the work done to complete the full scope of the safety case, including on non-reactor faults. Therefore, I have not identified the need for any specific Assessment Findings for a future licensee to address that are in addition to the 'normal business' of producing an adequate safety case to facilitate operations of a new nuclear power plant.

In summary, I am satisfied that GDA Issue GI-AP1000-FS-08 can be closed.

LIST OF ABBREVIATIONS

ALARP	As Low As Reasonably Practicable
ATWS	Anticipated Transient Without Scram
BDB	Beyond Design Basis
C&I	Control and Instrumentation
CCF	Common Cause Failure
CMT	Core Makeup Tank
DAC	Design Acceptance Confirmation
DAS	Diverse Actuation System
DB	Design Basis
DBA	Design Basis Analysis
GDA	Generic Design Assessment
HFLC	High-Frequency, Low-Consequence (faults)
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
IDAC	Interim Design Acceptance Confirmation
LOCA	Loss Of Coolant Accident
ONR	Office for Nuclear Regulation
PCS	Passive Containment Cooling (system)
PCSR	Pre-Construction Safety Report
PMS	Protection and Safety Monitoring System
PRHR	Passive Residual Heat Removal (system)
PSA	Probabilistic Safety Analysis
RNS	Normal Residual Heat Removal System
SAPs	Safety Assessment Principles
SSC	Structure, System and Component
TAG	Technical Assessment Guide
TSC	Technical Support Contractor
Westinghouse	Westinghouse Electric Company

TABLE OF CONTENTS

1 INTRODUCTION 7
1.1 Background 7
1.2 Overview of GI-AP1000-FS-08 7
1.3 Scope 8
1.4 Method 8
2 ASSESSMENT STRATEGY 9
2.1 Pre-Construction Safety Report 9
2.2 Standards and Criteria 9
2.3 Use of Technical Support Contractors 11
2.4 Integration with Other Assessment Topics 11
2.5 Out of Scope Items 12
3 REQUESTING PARTY'S DELIVERABLES IN RESPONSE TO THE GDA ISSUE 14
3.1 Chapter 8 of the PCSR 14
3.2 Hazard Schedules 17
4 ONR ASSESSMENT OF GDA ISSUE GI-AP1000-FS-08 18
4.1 The Adequacy of the 'Main' Fault Schedule 18
4.2 The Adequacy of the Supplementary Information Provided in Chapter 8 22
4.3 Internal and External Hazards 23
4.4 Assessment Findings 24
5 CONCLUSIONS 25
6 REFERENCES 26

1 INTRODUCTION

1.1 Background

1. Westinghouse Electric Company LLC (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 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 GDA Issues.

2. This report is the Office for Nuclear Regulation's (ONR's) assessment of the Westinghouse **AP1000** reactor design in the area of fault studies. Specifically, this report addresses GDA Issue GI-AP1000-FS-08 "Fault Schedule for **AP1000**".

3. The related GDA Step 4 report (Ref. 1) is published on our website (www.onr.org.uk/new-reactors/ap1000/reports.htm), and this provides the assessment underpinning the GDA Issue. Further information on the GDA process in general is also available on our website (www.onr.org.uk/new-reactors/index.htm).

1.2 Overview of GI-AP1000-FS-08

4. It is well-established good practice in the UK to summarise key aspects of a nuclear facility's safety case (in particular, the faults studies or design basis aspects) in a tabular form. This tabular summary is commonly referred to as a 'fault schedule'. There are wide variations in the scope, structure and format of fault schedules. ONR does not prescribe a format; it is for individual licensees and requesting parties to generate their own fault schedules that meet their objectives and reflect the facility / technology under consideration. However, most fault schedules share some common features:

   - The faults considered within the safety case are systematically and comprehensively identified.
   - The initiating event frequencies attributed to identified faults are indicated.
   - The major safety functions that need to be delivered following an individual fault are identified ('classically' control of reactivity, cooling and containment / confinement functions).
   - The Structures, Systems and Components (SSCs) claimed in the safety case as being available and effective to deliver the necessary safety functions following a fault, along with their safety classification, are identified.
   - References to where more detailed information and substantiation can be found to support the summary in the fault schedule entry are provided.

5. Westinghouse developed the **AP1000** design, together with supporting documentation, in the US where fault schedules are not routinely produced. During GDA Steps 3 and 4, ONR stressed to Westinghouse the importance of a good fault schedule to support the **AP1000** safety case. Ref. 1 details how Westinghouse provided a number of draft and provisional fault schedules during the original GDA process. However, Westinghouse only generated a final fault schedule at the end of GDA Step 4 as part of the Pre-Construction Safety Report (PCSR) (Ref. 2). This was too late for assessment and as a result ONR raised GDA Issue GI-AP1000-FS-08 requiring Westinghouse to:

   - submit a fault schedule to ONR;
   - support ONR's subsequent assessment of the fault schedule; and
   - update it as appropriate to address ONR comments and any relevant outcomes from addressing the other 50 GDA Issues.

1.3 Scope

6. The assessment plan (Ref. 3) details the scope of this assessment. Consistent with this plan, the assessment is restricted to considering whether the Westinghouse submissions to ONR for GI-AP1000-FS-08 provide a response sufficient to justify closure of the GDA Issue. As such, this report only presents the assessment undertaken as part of the resolution of this GDA Issue and it is recommended that this report be read in conjunction with the Step 4 fault studies assessment of the Westinghouse **AP1000** reactor (Ref. 1) to appreciate the totality of the assessment of the evidence in the fault studies safety case undertaken as part of the GDA process.

7. A good fault schedule should be an accurate summary of a facility's safety case. It would, therefore, be unusual for it to uniquely contain information that is not explained in more detail elsewhere. ONR assessed in detail Westinghouse's safety case for the **AP1000** reactor during GDA Steps 3 and 4. ONR judged it to be sufficiently adequate for an IDAC to be issued. Where significant gaps were found, GDA Issues and Assessment Findings were written for future resolution. The objective of my assessment for GI-AP1000-FS-08 is to establish that the objectives, structure and format of the fault schedule are adequate for GDA, and that its contents are consistent with the safety case. The adequacy of the safety case that the fault schedule is summarising has, therefore, been assessed elsewhere (notably Ref. 1 and ONR's assessment of the other 50 GDA Issues).

8. It is not ONR's role to be part of Westinghouse's verification process. As part of this assessment, I looked at preliminary versions of the fault schedule and brought to Westinghouse's attention errors or inaccuracies to address in subsequent revisions. I have commented on my overall impression of the quality and accurateness of the final version of the fault schedule based on a significant sample of key faults. However, I have not performed a line-by-line check of every entry in the fault schedule. It is assumed that the fault schedule, as an integral part of the PCSR, has been through Westinghouse's quality assurance process in accordance with its declared internal arrangements for GDA.

1.4 Method

9. This assessment has been undertaken consistent with internal guidance on the mechanics of assessment within ONR (Ref. 4).

2 ASSESSMENT STRATEGY

2.1 Pre-Construction Safety Report

10. ONR's GDA Guidance to Requesting Parties (Ref. 5) states that the information required for GDA may be in the form of a PCSR, and Technical Assessment Guide (TAG) NS-TAST-GD-051 sets out regulatory expectations for a PCSR (Ref. 6).

11. At the end of Step 4, ONR and the Environment Agency raised GDA Issue GI-AP1000-CC-02 (Ref. 7) 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.

12. A separate regulatory assessment report has been written to consider the adequacy of the PCSR and closure of GDA Issue GI-AP1000-CC-02, and therefore this report does not attempt to assess the totality of the **AP1000** PCSR. However, Westinghouse has chosen to make the fault schedule an integral part of the PCSR, effectively devoting all of Chapter 8 to it. By definition, the fault schedule (Chapter 8 of the PCSR) is a summary of other parts of the PCSR and provides links from accident analysis safety case claims (principally set out in Chapter 9 of the PCSR but also Chapters 10, 11, 12 and 13) to the various engineering chapters. This assessment report, therefore, provides a thorough review of Chapter 8 of the PCSR. In addition, its conclusions on the completeness, coherence and traceability of the fault schedule are relevant to ONR's assessment for GI-AP1000-CC-02 on the same characteristics as applied to the wider safety case.

2.2 Standards and Criteria

13. I have undertaken the assessment in line with the requirements of the HOW2 BMS document NS-PER-GD-014 (Ref. 8). In addition, the Safety Assessment Principles (SAPs) (Ref. 9) constitute the regulatory principles against which dutyholders' safety cases are judged, and, therefore, they are the basis for ONR's nuclear safety assessment. The SAPs 2014 Edition (Revision 0) has been used when performing the assessment described in this report (the original Step 4 fault studies assessment used the 2006 Edition).

2.2.1 Safety Assessment Principles and Technical Assessment Guides

14. The following SAPs (Ref. 9) were identified in the assessment plan (Ref. 3) as being appropriate to judge the adequacy of the arguments in the area of fault studies for the UK **AP1000** reactor.

- Fault Analysis SAPs FA.1 to FA.9
- Severe Accidents SAPs FA.15 and FA.16
- Engineering SAPs EKP.2 to EKP.5, ECS.1, ECS.2, EDR.1 to EDR.4, ESS.2, ESS.4, ESS.6 to ESS.9, ESS.11, ERC.1 to ERC.3, EHT.1 to EHT.4
- Computer Codes and Calculation Methods SAPs AV.1 to AV.8
- Numerical Target for DBA Consequences Target 4

15. It is important to note, however, that the scope of the assessment to close the GDA Issue is narrowly defined and is less than that of a typical ONR assessment, such as that undertaken in GDA Step 4. The original fault studies assessment (Ref. 1), which resulted in GI-AP1000-FS-08, considered the SAPs identified above. Also, as stated in Section 1.3, this assessment has not looked to assess the safety case claims contained within the fault schedule, just to determine that they accurately reflect more detailed arguments provided (and assessed) elsewhere.

16. Two SAPs specifically identify the expectations for a fault schedule:

ESS.11 – Demonstration of Adequacy	The adequacy of the system design to achieve its specified functions and reliabilities should be demonstrated for each safety system. *A fault schedule (sometimes known as a safety schedule or a fault and protection schedule) should be provided to link faults, fault sequences and safety measures (see Principle FA.8). For each initiating fault or event, the schedule should identify the relevant initiating fault frequencies, the potential fault consequences, the safety systems and administrative safety measures that provide protection, any beneficial safety-related systems, the mitigated fault sequence frequency and the overall protection claim. The fault schedule should also identify any passive safety measures claimed to prevent faults or mitigate their consequences.*
FA.8 – Linking of Initiating Faults, Fault Sequences and Safety Measures	Design Basis Analysis (DBA) should provide a clear and auditable linking of initiating faults, fault sequences and safety measures. *The analysis should demonstrate that:* *(a) all design basis initiating faults are addressed;* *(b) appropriate safety functions have been identified for the design;* *(c) the performance requirements for the safety measures have been identified; and* *(d) suitable and sufficient safety measures are provided.* *This demonstration should be summarised on a fault schedule.*

17. The expectations set out in ESS.11 and FA.8 are clear and to date ONR has not found it necessary to provide more detailed guidance on fault schedules in supporting TAGs.

18. TAG NS-TAST-GD-051 (Ref. 6) sets out some generic expectations for safety cases, including:

- All references and supporting information should be identified and be easily accessible.
- There should be a clear trail from claims through the arguments to the evidence that fully supports the conclusions, together with commitments to any future actions.
- A safety case should accurately represent the current status of the facility in all physical, operational and managerial aspects.
- There should be references out from the safety case to important supporting work, such as engineering substantiation. The safety case should be able to act as an entry point for accessing all relevant supporting information on which it is built.

19. Experience has demonstrated that a good fault schedule is a vital component of a safety case if these expectations are to be met.

2.2.2 National and International Standards and Guidance

20. The information that is shown on a fault schedule is consistent with that established by International Atomic Energy Agency (IAEA) standards as a requirement for demonstrating the safety of a nuclear power plant (Ref. 10), for example:

- Requirement 13: Categories of plant states – Plant states shall be identified and shall be grouped into a limited number of categories primarily on the basis of their frequency of occurrence at the nuclear power plant.
- Requirement 14: Design basis for items important to safety – The design basis for items important to safety shall specify the necessary capability, reliability and functionality for the relevant operational states, for accident conditions and for conditions arising from internal and external hazards, to meet the specific acceptance criteria over the lifetime of the nuclear power plant.
- Requirement 16: Postulated initiating events – The design for the nuclear power plant shall apply a systematic approach to identifying a comprehensive set of postulated initiating events such that all foreseeable events with the potential for serious consequences and all foreseeable events with a significant frequency of occurrence are anticipated and are considered in the design.
- Requirement 19: Design basis accidents – A set of accidents that are to be considered in the design shall be derived from postulated initiating events for the purpose of establishing the boundary conditions for the nuclear power plant to withstand, without acceptable limits for radiation protection being exceeded.
- Requirement 22: Safety classification – All items important to safety shall be identified and shall be classified on the basis of their function and their safety significance.

21. However, the need to summarise this type of information in a schedule is UK good practice that is not generally followed elsewhere. The SAPs (and not the international references) are, therefore, the foremost standards considered in this assessment.

2.3 Use of Technical Support Contractors

22. No Technical Support Contractors (TSCs) have been used in this assessment.

2.4 Integration with Other Assessment Topics

23. A comprehensive fault schedule should summarise large portions of a facility's safety case and is of interest / relevance to almost all ONR assessment topic areas. It can provide a key interface tool between the engineering disciplines and the safety analysis areas (notably fault studies), allowing the different areas to quickly converge on the key safety claims that are important to their assessments.

24. Westinghouse has supplied several revisions of its fault schedule to ONR since its return to the GDA process. I ensured that these were widely circulated to all ONR assessment topic areas, with a request to relay any feedback or issues back to me for further discussion with Westinghouse. In addition, Westinghouse provided a presentation to a cross-discipline audience of ONR inspectors on an early version of its fault schedule. It explained the purpose, scope, structure and content of its fault schedule, and responded to comments as appropriate. This presentation was a major part of Westinghouse's declared commitment for GDA Issue resolution to support ONR's assessment of the fault schedule.

25. A significant area of co-operation has been between the fault studies and internal hazard topic areas. ONR expects internal (and external) hazards to be treated as

potential initiators for design basis events (SAP EHA.3), with the safety case clearly demonstrating that the expectations of SAPs ESS.11 and FA.8 are met. The conclusion of ONR's GDA Step 4 fault studies assessment (Ref. 1) was that internal and external hazards were not presented within the list of design basis initiating events produced by Westinghouse in response to a Regulatory Observation (RO) (Ref. 11) and therefore it was difficult to see whether the barriers protecting against the fault were appropriately categorised and classified. As a result, Ref. 1 set an explicit requirement for Westinghouse to include consideration of internal and external hazards in its response to GDA Issue GI-AP1000-FS-08.

26. There are no external hazards GDA Issues and therefore the safety case in that area has been effectively fixed since Westinghouse's return to the GDA process. Given that I am not considering the substantiation of safety case claims in this assessment (instead focusing on whether the fault schedule accurately reflects the extant safety case), I have come to my own judgements on the adequacy with which external hazards are included in the fault schedule (with some limited advice from specialist colleagues).

27. In contrast, the internal hazards topic area has been very active since Westinghouse's return to GDA, with six GDA Issues actively addressed and major revisions of the relevant sections of the PCSR made. I have worked closely with internal hazards colleagues to ensure the work done for GI-AP1000-FS-08 is fully integrated and consistent with the developing safety case in their area.

2.5 Out of Scope Items

28. I have already stated the major scope limitation for this assessment. To allow me to close this GDA Issue, I have looked for evidence that the fault schedule accurately and comprehensively summarises the relevant aspects of the extant safety case for the **AP1000** reactor, including work undertaken to close the other 50 GDA Issues. However, I have assumed the adequacy of the underlying safety case arguments that the fault schedule summarises has been assessed elsewhere.

29. I have taken cognisance of the full scope of safety case areas covered by Westinghouse in its fault schedule. However, for my detailed assessment to inform GDA Issue closure, I have focused on three main portions of the fault schedule that summarise areas of the safety case that have been subject to extensive ONR review:

- reactor faults (in all operating modes) as described in Chapter 9 of the PCSR
- internal hazards as described in Chapter 11 of the PCSR
- external hazards as described in Chapter 12 of the PCSR

30. Notably, I have largely excluded from detailed consideration fault schedule entries for fuel route, dropped loads, waste management and other non-reactor faults. It is appropriate that these faults appear in the fault schedule, and I will make some comment on the relevant entries in Section 4 of this assessment, but it is my judgement that a mature fault schedule in these areas is not necessary for closing this GDA Issue. This is informed by the fact that ONR's GDA Step 4 control and instrumentation (C&I) assessment (Ref. 13) excluded from its declared scope all platforms and systems important to safety associated with lifting equipment and the waste treatment building C&I. Given that ONR specialists have not looked at the safety case in those areas, it would not be proportionate or appropriate to challenge the closure of GDA as a result of an assessment of a summary of part of the **AP1000** safety case that has been excluded from GDA consideration.

31. Ref. 13 raised an Assessment Finding (AF-AP1000-CI-004) for a future licensee to 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.

32. It goes on to state that the Assessment Finding 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.

33. The fault schedule should be a living document. When a future licensee addresses AF-AP1000-CI-004, I expect that the fault schedule will be updated appropriately to reflect the outcome of the work. Therefore, the portion of fault schedule that has been excluded for detailed review in GDA is expected to be extensively revised during site licensing.

3 REQUESTING PARTY'S DELIVERABLES IN RESPONSE TO THE GDA ISSUE

34. Westinghouse's principal submission to address this GDA Issue is Chapter 8 of the PCSR. This chapter is dominated by Appendix 8A "Fault and Accident Analysis: **AP1000** Composite Fault List", (which is what Westinghouse has chosen to call its fault schedule) but it also contains other tables, figures and text which I will describe below.

35. Discussions with Westinghouse on this GDA Issue initiated with the version of the fault schedule generated at the end of GDA Step 4 and contained in the March 2011 PCSR (Ref. 2). Over a period of circa two years, various drafts and formal updates of the fault schedule and Chapter 8 of the PCSR were supplied to ONR for assessment and feedback. Ultimately, this report describes judgements reached based on a review of the contents of the final version (Revision 1) of the GDA PCSR supplied in January 2017 (Ref. 12).

36. As part of its GDA Issue work in the internal hazards topic area, Westinghouse has written six topic reports describing the **AP1000** reactor's safety case for the following:

- fire hazards
- internal flooding hazards
- pressure part failure
- explosions
- internal missiles
- dropped loads

37. Each of these topic reports includes a 'hazard schedule' that summarises in tabular form the safety case for individual areas, systems and operations for the hazard under consideration. These hazard schedules have been consolidated in Chapter 11 of the PCSR (Ref. 12). Westinghouse has identified these hazard schedules as being sources of complementary information to Chapter 8 fault schedule entries for internal hazards of the PCSR. I have therefore considered them to be part of Westinghouse's submissions for this GDA Issue.

3.1 Chapter 8 of the PCSR

3.1.1 Overview

38. The main part of Chapter 8 (ie not the Appendix containing the fault schedule) explains how subsequent sections of the PCSR (including the fault schedule) will demonstrate that the **AP1000** reactor has an adequate safety case for faults and accidents.

39. It states that the objectives for the safety case are to demonstrate that the provision of Category A safety functions is sufficient to meet regulatory targets and As Low As Reasonably Practicable (ALARP) risk reduction expectations for at least the first 72 hours following any abnormal event and Category B safety functions post 72 hours. For the reactor, it states that the main Category A safety functions are reactivity control, decay heat removal and containment.[1]

40. Chapter 8 goes on to say:

- Westinghouse has followed a systematic, auditable, and comprehensive process to identify faults. This includes internally initiated faults, internal hazards, external hazards, and human errors. It also includes all modes of normal operation of the reactor and radioactive inventories in other areas (the

[1] *Westinghouse has also identified containment cooling, containment isolation, pressure control and "SSC support" as required safety functions. The first two of these appear directly in the fault schedule, the second two functions are dealt with outside of the fault schedule.*

spent fuel in the auxiliary building and waste routes, in particular). These faults are listed in the fault schedule.

- Each fault has been allocated a design basis (DB) class based on the initiating event frequency. The DB classes are based on ONR's Target 4 set out in the SAPs:
  - DB1 – infrequent DB faults with an initiating event frequency between $1x10^{-3}$ per year and $1x10^{-5}$ per year.
  - DB2 – frequent DB faults with an initiating event frequency $>1x10^{-3}$ per year.
  - DBL – low probability DB faults with an initiating event frequency between $1x10^{-5}$ per year and $1x10^{-6}$ per year (and consequences limited to public dose < 200 mSv or worker dose < 1000 mSv).
  - BDB – beyond design basis (BDB) faults with an initiating event frequency $<1x10^{-6}$ per year, ie below the frequency for DBL faults but with consequences that would be higher than for DBL events.
  - HFLC – High-frequency, low-consequence (HFLC) faults initiating event frequency $>1x10^{-3}$ per year with consequence limits between DB limits and normal operating limits.
  - DB0 – All other faults; no radiological consequences expected.

- The DB class, together with the categorisation and classification scheme given in Chapter 5 of PCSR, defines the requirements for safety measures:
  - DB2 – Two diverse mitigation capabilities are required for each Category A safety function. At least one capability must be Class 1. The other may be Class 2. Analysis of the plant with consideration for a common cause failure may be performed with less conservative methods and/or inputs and may apply relaxed acceptance criteria.
  - DB1 – One Class 1 mitigation capability is required for each Category A safety function.
  - DBL – One Class 1 mitigation capability is required for each Category A safety function. Analysis of the plant may be performed with less conservative methods and/or inputs and may apply relaxed acceptance criteria.
  - HFLC – No formal requirement, but best practice is to identify one Class 2 system for each Category B safety function.
  - BDB – No formal requirement except for demonstrating event considerations are ALARP.
  - DB0 – No formal requirement except for demonstrating event considerations are ALARP.

- Analysis to support the design basis safety case for internally initiated events, internal hazards, external hazards and human errors is provided in Chapters 9, 11, 12 and 13 respectively of the PCSR.
- The design basis safety case, along with the Probabilistic Safety Analysis (PSA) and severe accident analysis in Chapter 10 are used to show that deterministic and probabilistic targets are met (and that the design is ALARP).
- The requirements placed on engineered systems during fault and accident conditions and the evidence that they can meet these requirements are provided elsewhere in the PCSR, notably the engineering schedule included in Chapter 15.

41. This information is important for setting the context for the fault schedule and Westinghouse's ambitions for it in support of the safety case. The fault schedule itself is provided in Appendix A alongside other relevant information:

- Introductory text explains what Westinghouse's fault schedule presents.

- Table 8A-1 defines the different operating modes considered in the **AP1000** safety case (and therefore the fault schedule).
- Table 8A-2 is the main fault schedule for the **AP1000** reactor (titled “composite fault list for reactor internal and non-internal events and internal and external hazards”).
- Table 8A-3 is a less detailed and higher level fault list specifically for decommissioning and dry spent fuel storage faults.
- Table 8A-4 lists the support systems (for example C&I, electrical power and heating and ventilation) for the frontline SSCs listed in Table 8A-2 as delivering safety functions.
- Table 8A-5 lists the SSCs needed for long-term passive system support (ie after 72 hours).

42. The main fault schedule (Table 8A-2) is described further in the section below.

3.1.2 Fault Schedule

43. The fault schedule presented in Table 8A-2 (Ref. 12) is built upon an extensive list of initiating faults that Westinghouse claims are addressed by the PCSR. It runs to circa 50 pages and therefore the faults have been broken up into five sections:

Section 1 – reactor internal events
Section 2 – additional reactor internal faults
Section 3 – non-reactor faults
Section 4 – internal hazards
Section 5 – external hazards

44. Further subdivisions are made within each section (for example, Section 1 has 1.1 “RPV rupture events”, 1.2 “Large LOCA”, 1.3 “Interfacing system LOCA”), with the individual faults being allocated a three-level unique fault identification number based on the subdivision it falls within (for example, 1.1.1, 1.2.1, 1.2.2).

45. The fault schedule table has multiple columns, such that for each individual fault, the following information is provided:

- The unique fault identification number.
- A brief description of the fault.
- The consequences that result from the fault progressing.
- The initiating event frequency and DB class of the fault.
- The reactor operating mode(s) the fault is applicable in (as defined in Table 8A-1).
- The frontline SSCs that are claimed to maintain the essential safety functions of reactivity control, heat removal and containment of radioactive material following the fault (for up to 72 hours). The parameter which prompts the initiation of a claimed SSC is indicated, as well as whether that initiation is automatic or manual. The safety classification of both the initiation signals and the SSC delivering the safety function.
- A comments section providing additional relevant details.
- A reference to where further safety case information and analysis can be found (usually Chapters 9, 10, 11 or 12 of the PCSR).

46. For DB1 and DBL faults, a single set of SSCs is identified to deliver the necessary essential safety functions of reactivity control, heat removal and containment following the fault. These are almost exclusively Class 1 passive SSCs that can provide at least 72 hours of operation. After 72 hours, additional support is needed from the ancillary systems identified in Table 8A-5.

47. For DB2 faults, Westinghouse has set itself the objective of showing that there are two diverse means of providing Category A safety functions following the fault. It has used coloured shading to identify the different SSCs being claimed:

- SSCs in unshaded (or white) boxes are the primary means of delivering the necessary safety functions.
- SSCs in grey shaded boxes are those claimed in the design basis safety case as being effective assuming a Common Cause Failure (CCF) of the primary means of delivering the heat removal safety function and long-term reactivity control.
- SSCs in blue shaded boxes are those claimed in the design basis safety case as being effective assuming a CCF of the primary means of providing short-term reactivity control (ie in the event of failure to trip the reactor, often referred to as an Anticipated Transient Without Scram or ATWS).

48. For most DB2 faults, the fault schedule shows that diverse Class 1 passive SSCs are available to deliver the necessary essential safety functions. However, there are many claims on the Class 2 Diverse Actuation System (DAS) to initiate the Class 1 SSCs. In the case of small break Loss Of Coolant Accidents (LOCAs), there is also a claim on the Class 2 Normal Residual Heat Removal System (RNS).

3.2 Hazard Schedules

49. All six hazard schedules written in support of the internal hazards GDA Issue closure and included in Chapter 11 of the PCSR (Ref. 12) have broadly similar structures. The following information is generally provided (there are variations in format from schedule to schedule):

- The specific location being considered.
- The source or cause of the internal hazard in that particular location.
- The SSCs in that location that deliver essential safety functions and could be lost if the internal hazard is not protected against.
- The unmitigated consequences that could occur if the internal hazard occurred, including a reference to any applicable design basis fault in the fault schedule.
- The safety features claimed in the internal hazards safety case that prevent the unmitigated consequences from occurring (including the safety function the features provide and their safety classification).
- Any redundant means of delivering the same essential safety functions provided by the SSCs potentially threatened by a hazard in the location under consideration.
- Any additional defence-in-depth means of protecting against the hazard, in addition to main safety features claimed.
- The (mitigated) consequences of the internal hazard if the claimed safety measures are effective (usually none, or less severe than the design basis event identified in the fault schedule).
- Additional notes and comments as appropriate.

4 ONR ASSESSMENT OF GDA ISSUE GI-AP1000-FS-08

50. My assessment of Westinghouse's submissions for GI-AP1000-FS-08 is set out below, against the scope defined in Section 1 and strategy discussed in Section 2.

51. I have broken my assessment into three subsections:

- The adequacy of the 'main' fault schedule provided in Table 8A-2 of Ref. 12.
- The adequacy of the supplementary information provided in Chapter 8 of Ref. 12 that is associated with the fault schedule.
- The adequacy with which the fault schedule and hazard schedules together address the requirements of the GDA Issue for internal and external hazards.

52. As has previously been stated, the judgements reported on the adequacy of Westinghouse's work to close the GDA Issue are based on a review of the referenced submissions. However, they are informed by many meetings and months of interactions with Westinghouse on preliminary versions of the fault schedule.

4.1 The Adequacy of the 'Main' Fault Schedule

4.1.1 Format of the Fault Schedule

53. There is no one prescribed format for a fault schedule. Licensees and requesting parties choose different formats based on the reactor / facility technology they are responsible for, the specific faults and safety functions being considered, the approach their wider safety case takes, the information provided elsewhere in other documents (eg engineering or hazard schedules, if they exist), or in some cases simply the safety case author's preferences. It is almost always a compromise, taking into account what information would be useful to a reader / user and what can be practically fitted into table that is legible when printed out.

54. Westinghouse developed its fault schedule format during GDA Step 4 through discussion with ONR (noting that a final, completed fault schedule was not submitted in time for formal ONR assessment). The final version submitted in Table 8A-2 of Ref. 12 is essentially unchanged (with respect to the columns and their titles) from GDA Step 4.

55. I am satisfied that the format Westinghouse has chosen is adequate for its technology and is consistent with relevant good practice for internally initiated events and hazards that affect the reactor. It is worth noting that Westinghouse has chosen to reference out to supporting tables to identify which supporting systems are required in the short term and beyond 72 hours (Tables 8A-4 and 8A-5 respectively of Ref. 12). I have no objections or concerns with this approach.

56. I am also satisfied that Westinghouse's approach for describing loss of water or active cooling faults for the spent fuel pool with the fault schedule format is acceptable. However, for the vast majority of non-reactor faults, Westinghouse has stated "N/A" (not applicable) in many of the columns for essential safety functions. I will comment later about the adequacy of the fault schedule for non-reactor faults; however, I can envisage some advantages in separating out non-reactor faults from the main fault schedule and adopting a different format for identifying and classifying SSCs that are delivering essential safety functions for these events. Westinghouse has not done this but I judge that this is not an impediment to any decision to close the GDA Issue.

4.1.2 Scope of the Fault Schedule

57. Westinghouse states in Ref. 12 that the fault schedule includes internally initiated faults, internal hazards, external hazards and human errors. It is also intended to include all modes of normal operation of the reactor and radioactive inventories in

other areas (the spent fuel in the auxiliary building and waste routes). It is my view that this is an entirely appropriate scope for a fault schedule.

58. During GDA Step 4, ONR's fault studies assessment considered the completeness of the list of design basis reactor and spent fuel pool faults considered in the **AP1000** safety case (Ref. 1). This included a comparison against the list of faults considered in Westinghouse's PSA. The conclusion of this previous review was broadly positive, with the requirement to fill any gaps being captured by other fault studies GDA Issues or Assessment Findings.

59. I am satisfied that the fault schedule in Ref. 12 includes all the appropriate design basis reactor and spent fuel pool faults identified as appropriate during GDA Step 4, and that it also includes additional faults identified through addressing the other fault studies GDA Issues. I do not expect that the fault schedule contained within the GDA PCSR pre-empts the outcomes of future licensee work on Assessment Findings.

60. I am also satisfied that Westinghouse has adequately identified appropriate internal and external hazards that need to be considered in the fault schedule for GDA (a review during site licensing will be necessary to reflect the hazards particular to the location proposed for **AP1000** reactor construction in the UK). Westinghouse has chosen to demonstrate that it has systematically considered the impact of the identified hazards on a specific system or location in Chapters 11 and 12 of the PCSR and supporting references (including the hazard schedules). Only bounding design basis hazard sequences are presented in the fault schedule. The fault schedule does not list all the design features identified in the internal hazards safety case that make a contribution to safety. Instead, it has just identified the systems that maintain reactor safety should the hazard occur, with no reference to the low classification SSCs which are designed to prevent or minimise the consequences of an internal hazard. This is an acceptable approach, which is discussed further in Section 4.3. The completeness and adequacy of the safety case for internal and external hazards, which the fault schedule is designed to summarise (ie Chapters 11 and 12 of the PCSR), are beyond the scope of this fault studies assessment.

61. I have been able to confirm that the fault schedule does include many non-reactor faults associated with buildings and operations with radioactive inventories. The list of faults included by Westinghouse is extensive and appears reasonable. However, the completeness of this list was not assessed during GDA Step 4 (by any technical discipline, not just fault studies) and it has not been a regulatory priority for me to pursue this to close the GDA Issue. While the reactor and spent fuel pool designs (and therefore the related faults included in the fault schedule) are anticipated to be largely invariant between the GDA process and the final facilities built on a UK site, there could be significant variations in radwaste facilities and maintenance practices depending on the final detailed design, the sharing of functions on a multi-unit site and a licensee's preferences / requirements. I am content with the precedent set by the GDA work that non-reactor faults are included with the scope of an **AP1000** fault schedule. I assume that the relevant entries will be reviewed and updated as necessary in accordance with a future operator's normal safety case arrangements during site licensing.

62. Westinghouse has not restricted the initiating events in the fault schedule to design basis events (ie DB1 and DB2) events. It has also included events it has classified as DBL, BDB, HFLC and DB0 that are outside of the traditional design basis region defined by Target 4 in the SAPs. I consider this to be an acceptable approach and, by doing the following, it helps Westinghouse to both demonstrate the completeness of its fault identification process (as set out in SAPs FA.2 and FA.5) and the generic safety properties set out in NS-TAST-GD-051 (Ref. 6):

- For further information on DB1 and DB2 events, the fault schedule entries point to references in Chapter 9 of the PCSR (the fault studies chapter describing the safety case for design basis internally initiated events).
- For further information on DBL events, the fault schedule entries generally point to references in Chapters 9 and 10 (the PSA chapter) of the PCSR.
- For further information on BDB events, the fault schedule entries generally point to references in Chapter 10 of the PCSR.
- There are only two examples of HFLC events. In one case, both Chapters 9 and 10 are referenced, in the other just Chapter 9 is referenced.
- The listed DB0 events are almost exclusively associated with non-reactor faults. Some of the events are screened out from further discussion based on their consequences while others point to Chapter 9 for more information.

63. Although Westinghouse has chosen to extend the list of initiating events included in the fault schedule to beyond the traditional design basis, it has only identified the SSCs that are claimed in the design basis safety case to deliver essential safety functions. It has also chosen not to systematically present the control systems that would be normally expected to manage a transient before a demand is placed on a design basis safety system, nor any additional defence-in-depth systems that could contribute to safety (ie systems which are credited in the PSA but not the design basis safety case). Some fault schedules do show this level of information (consistent with SAP ESS.1); however, I do not object to Westinghouse excluding them, and note that the design basis focused expectations of SAP FA.8 are fully met. I also note that for many reactor faults, the ALARP discussion in Chapter 9 of the PCSR often summarises the available defence-in-depth systems for faults, and the PSA includes these extra features.

4.1.3 Visibility of SSCs Delivering Safety Functions

64. Clearly identifying the SSCs that are claimed in the design basis safety case to deliver essential safety functions (and detailing the safety classifications of those SSCs) is a fundamental objective for most fault schedules.

65. Westinghouse's fault schedule for the **AP1000** plant demonstrably provides this information for reactor and spent fuel pool faults (including hazards). For all DB1, DB2 and DBL faults (and most BDB faults) the SSCs that provide the identified safety functions are identified along with their safety classification. In addition, the C&I platform that initiates the safety function delivering SSC is identified, along with its safety classification and whether the initiation is automatic or manual.

66. In most cases, the plant parameter assumed in the support transient analysis to prompt a C&I initiation signal is also identified. There are few entries in the fault schedule where the plant parameter is not specified. Westinghouse stated in response to a Regulatory Query that it has excluded this level of information in cases where the consequences of a fault sequence have been bounded by analysis or arguments from other faults (or the same fault in a different operational mode), and therefore it does not have information to identify which of potentially numerous prompts would initiate specific SSCs (Ref. 14). I am content with this approach, noting that as a result of Ref. 14 it has expanded the supporting text in the final version of Chapter 8 (Ref. 12) to provide additional explanations for when details of the trip parameter are provided.

67. Many reactor faults are clearly more limiting if they occur at full power than in shutdown modes because the associated pressures, temperatures and decay heat levels experienced during the transient are higher. However, in (shutdown) operating modes 3 to 6 it is permissible / required to take out of service some of the SSCs identified by safety case for at-power (modes 1 and 2) operating modes. Therefore, the safety case arguments and analysis demonstrating the safety of the **AP1000** plant undertaken for modes 1 and 2 are not automatically applicable to lower modes. Westinghouse has addressed this in the fault schedule by breaking faults into different

entries when there is a reduced (or different) claim on the availability of SSCs, depending on the operating mode. I consider this to be a sensible and powerful approach for Westinghouse to demonstrate that it has an adequate safety case for all operating modes. This meets its objectives for its fault schedule. When taken together with the information on Class 1 availability in different operating modes in Table 9.8.3-1 of the PCSR (Ref. 12), the Tier 1 Technical Specifications (Ref. 15), and the Tier 2 Technical Requirements Manual (Ref. 16), it meets ONR's expectations in SAP FA.6 for a safety case to cover all permitted plant states.

68. As described in Section 3, for frequent faults (DB2), Westinghouse has demonstrated that it has diverse means of delivering the essential safety functions, with a colour scheme separating out the diverse cooling sequences from the ATWS sequences. For most at-power cases, it has provided two entries for the diversity demonstration (an ATWS sequence is not needed for shutdown faults so only one entry is required in those cases). However, for some faults (notably small break LOCA faults), it has artificially split the fault sequences into unlikely but demonstrably effective combinations of SSCs that are each functionally capable of delivering all the necessary safety functions. This results in some entries that are difficult to interpret at first glance, but I am satisfied that through the appropriate discussion supplied in the accompanying 'comments' column and by following the identified reference trail provided for each entry, a fault schedule user can establish what the **AP1000** safety case is for DB2 faults.

69. Given the observations above, I judge that Westinghouse's fault schedule provides adequate visibility of the SSCs claimed in the design basis safety case which protect against reactor and spent fuel pool faults. This, along with the completeness of the list of faults it includes, is a key aspect for reaching a positive conclusion about closing this GDA Issue. However, the fault schedule does not generally give a good level of detail on the SSCs that are important to the safety case for non-reactor faults. While many relevant faults are identified, their radiological consequences are characteristic of DB0 and no further consideration is given. In most cases, this is not because the consequences or initiating event frequency are intrinsically limited by the nature of the event or size of the source term. Rather, it is because of one or more engineered features (eg crane protection systems which prevent dropped loads or travel over vulnerable areas) are assumed to be effective in most design basis events. The extant fault schedule in Ref. 12 does not identify these SSCs, which are an important part of the safety case.

70. As stated in Section 2.5, I do not view the fault schedule's weakness in summarising the safety case for fuel route, dropped loads, waste management and other non-reactor faults as an impediment for closing this GDA Issue because large portions of the safety case in these areas have been excluded from consideration in GDA. The fault schedule, as a 'living' document, should be updated as the safety case is developed during site licensing and relevant Assessment Findings are addressed. I am content for the necessary improvements to be made through the future licensee's normal safety case arrangements.

4.1.4 Accuracy and Completeness of Information in the Fault Schedule

71. I have not verified every entry in the fault schedule, but as stated in Section 1.3, I have extensively sampled preliminary versions of the fault schedule and have informed Westinghouse of any inconsistencies or errors found. This sampling has been largely driven by the assessment of the fault sequences considered in the other fault studies GDA Issues: GI-AP1000-FS-01 through GI-AP1000-FS-07.

72. Given its length, some minor errors in the fault schedule are almost inevitable. However, my general impression is that fault identification numbers, fault descriptions, claimed SSCs and identified references for further information are accurate in the final

version supplied in Ref. 12. I am therefore satisfied that it is a sufficiently accurate summary of the design basis safety case (DB2, DB1 and DBL faults) as set out in Chapter 9 of the PCSR. I have not systematically followed the links identified for BDB and DBL faults to Chapter 10 (PSA). However, based on the findings of my Chapter 9-focused sampling and a presumption that Westinghouse has followed its internal quality assurance process, I have confidence that the links from BDB and DBL entries to the Chapter 10 safety case discussion should also be sufficiently accurate.

73. The fault schedule provides a cell for initiating event frequency and DB class for every fault. An exemplary fault schedule could provide explicit references for every frequency listed (eg in the PSA). Westinghouse's fault schedule does not do this. In the supporting text in Chapter 8, there is a generic explanation that the presented frequencies are taken from the PSA. In many cases, it is possible to follow the fault schedule entry through to the supporting Chapter 9 or 10 references, which gives specific information on the origins of the attributed initiating event frequency. Some faults have very precise initiating event frequencies suggesting they are substantiated by analysis. Others are clearly judgements limited to an order of magnitude (eg $>1x10^{-3}$ per year). For the purposes of GDA and closing this GDA Issue, I have not looked to ensure a traceable origin for every single initiating event frequency or consistency with the PSA, unless it has specific implications for the safety case treatment for a fault. The frequencies / DB class applied by Westinghouse to the major design basis faults were assessed during GDA Step 4 (Ref. 1) and as part of this assessment I have not discovered anything that challenged the conclusions of this earlier assessment.[2]

74. Regulatory Query RQ-AP1000-1788 is an example of the challenge on accuracy I have put to Westinghouse as a result of examinations of interim versions of the fault schedule. I am satisfied with Westinghouse's response (Ref. 14) and the subsequent updates made to the fault schedule in response to my comments and its own internal reviews. Ultimately, I am satisfied that the final version of the fault schedule produced for Chapter 8 of the PCSR (Ref. 12) is sufficiently complete and accurate for the closing of the GDA Issue.

4.2 The Adequacy of the Supplementary Information Provided in Chapter 8

75. As described in Section 3, Westinghouse has supplied a significant amount of supplementary text in Chapter 8 to support the main fault schedule. A fault schedule can only ever supply a summary of a much more extensive and detailed safety case, and some information is inevitably left out.

76. I consider the supporting text to be useful, indeed vital, information for the fault schedule and welcome its inclusion. There are particularly useful explanations on Westinghouse's approach to:

- the interface with the internal and external hazards safety case;
- specific details of the approach to demonstrating diversity for frequent internal fires;
- the extent to which the claimed SSCs have requirements on support systems such as power, cooling water and Heating, Ventilation and Air Conditioning (HVAC); and
- pressure control, containment cooling and containment isolation.

77. I also welcome the inclusion in Chapter 8 of the additional tables on:

- definition of operating modes (Table 8A-1)

[2] *There are two notable examples where the initiating event frequencies in the fault schedule have important safety case implications. The first is the frequency attributed to small break LOCAs. This has been looked at outside of this report as part of the assessment of GI-AP1000-FS-05. The other is the frequency attributed to spurious ADS-4 actuation. This has been looked at as part of the assessments of GI-AP1000-ME-01 and GI-AP1000-CI-04.*

- support systems for frontline SSCs (Table 8A-4)
- SSCs needed for long-term passive system support (Table 8A-5)

78. Table 8A-5 makes the significant claim for the generic **AP1000** design that the principal means of delivering long-term support (ie after 72 hours) for the passive SSCs assumed in the safety case is by equipment from off site. There is Class 2 ancillary equipment installed on site (for example, ancillary diesel generators) to deliver the same post-72-hour support functions; however, it is assumed to be a backup to the offsite equipment. A future licensee will need to look at how or if this claim can be substantiated during site licensing, taking into account local factors and the strategy for emergency arrangements adopted. However, for the purposes of closing out this GDA Issue, I am satisfied that Westinghouse's safety case assumptions are clearly set out.

4.3 Internal and External Hazards

79. As stated in Section 2.4, ONR's GDA Step 4 fault studies assessment (Ref. 1) observed that internal and external hazards were not presented within the list of design basis initiating events produced by Westinghouse in response to a Regulatory Observation (Ref. 11). Therefore, it was difficult to see whether the barriers protecting against the hazards were appropriately categorised and classified.

80. Internal and external hazards do appear in the fault schedule supplied in response to this GDA Issue and they are discussed extensively in the accompanying text in Chapter 8 (Ref. 12). All the entries for hazards are effectively claiming the same Class 1 passive SSCs that are fundamental to the **AP1000** design for intact circuit faults: the Passive Residual Heat Removal (PRHR) system, the Core Makeup Tanks (CMTs), containment isolation and the Passive Containment Cooling System (PCS), all initiated by the Protection and Safety Monitoring System (PMS). This unambiguously means that these SSCs need to be qualified to deliver their safety functions assuming that the most limiting variation of the considered design basis hazard has occurred. I am satisfied that this is not a new claim and is fundamental to the internal and external hazard safety cases presented in Chapters 11 and 12 of the PCSR (and assessed by ONR during GDA Step 4). To what extent this claim has been substantiated for all hazards is beyond the scope of this assessment report.

81. The fault schedule identifies that some design basis hazards should always be considered as frequent (eg fires), while variations of limiting (infrequent) design basis hazards could occur with less severe consequences on a more frequent basis (eg seismic events or wind events). Westinghouse has used the fault schedule to demonstrate that the **AP1000** reactor has diverse safety provision for these frequent external hazards. It has largely been able to make its safety case by putting claims on alternative Class 1 SSCs to those identified as the primary means of protection. These Class 1 SSCs are qualified for the limiting design basis hazards and are therefore qualified for the less severe versions of the hazard assumed to occur more frequently. The exception to this diverse Class 1 capability is a reliance on the Class 2 DAS to initiate the diverse Class 1 SSCs in the event of a failure of the PMS. Westinghouse has provided further discussion on the implications of these claims on the DAS in the main text of Chapter 8 (Ref. 12), including the potential for a fire to disable the DAS. Ultimately, I am satisfied that the claims made on diverse SSCs to deliver the necessary essential safety functions in the event of a frequent hazard are clear.

82. By definition, external hazards are beyond the control of the operators of a nuclear power plant. In contrast, Westinghouse as the designer of the **AP1000** plant, can give future operators the means to prevent, control or mitigate the consequences of internal hazards. However, symptomatic of the lack of a mature fault schedule or hazard schedule, it was not clear to ONR at the end of GDA Step 4 which SSCs were being claimed for these purposes and how important they were to the safety case (Ref. 1). I judge that the hazard schedules provided in Chapter 11 of the PCSR (Ref. 12) address

this shortfall. Although they are not part of the fault schedule, the hazard schedules provide a similar function that complements the main table in Chapter 8 of the PCSR. In addition to showing a systematic consideration of each hazard (as per SAPs EHA.1, FA.2 and FA.5) and giving references to further information, the principal means and any defence-in-depth means of controlling internal hazards are clearly indicated. Significantly, the hazard schedules show that many of the measures identified to minimise hazards or prevent them from occurring are designated as Class 3 SSCs delivering Category C safety functions. However, barriers to protect against the consequences of (for example) floods and some explosions are designated as Class 1 SSCs delivering Category A safety functions. Crucially, I consider that this presentation of a previously missing graded approach (linked to and consistent with the fault schedule) is adequate for the requirements of this GDA Issue. Again, the assessment of the internal hazards safety case that the hazard schedules are summarising and any judgements on whether the individual SSCs have been substantiated to deliver the identified safety functions under the conditions they will experience during a hazard is beyond the scope of this assessment report.

4.4 Assessment Findings

83. Assessment Findings are matters that 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.

84. Residual matters are recorded as Assessment Findings if one or more of the following apply:

- site-specific information is required to resolve this matter;
- the way to resolve this matter depends on licensee design choices;
- the matter raised is related to operator-specific features / aspects / choices;
- the resolution of this matter requires licensee choices on organisational matters;
- to resolve this matter, the plant needs to be at some stage of construction / commissioning.

85. In my assessment, I did not find any examples of matters that meet these criteria.

86. Many Assessment Findings already exist, either from the original GDA Step 4 assessment, or ONR's assessment work to close the other 50 GDA Issues. A significant portion of these are likely to result in changes to the safety case that will need to be reflected in future fault schedules. Of particular note is AF-AP1000-CI-004 (Ref. 13) that was discussed in Section 2.5 and requires a future licensee to review the classification of C&I equipment important to safety used in cranes and mechanical handling equipment.

5 CONCLUSIONS

87. This report presents the findings of the assessment of GDA Issue GI-AP1000-FS-08 relating to the AP1000 GDA closure phase.

88. As a result of my assessment of Westinghouse's submissions for this GDA Issue, notably the fault schedule included in Chapter 8 of the PCSR and hazard schedules included in Chapter 11 of the PCSR (Ref. 12), I have reached the following conclusions:

- Westinghouse has produced a fault schedule with a format and scope that is both appropriate for its technology / safety case and is consistent with relevant good practice.
- Based on an extensive sample of reactor faults, the fault schedule is an adequate summary of the design basis safety case (DB2, DB1 and DBL faults) set out in Chapter 9 of the PCSR (Ref. 12) and it provides a useful 'starting point' for understanding the beyond design basis safety case typically detailed in Chapter 10 of the PCSR.
- The fault schedule, complemented by hazard schedules, provides appropriate visibility to the graded approach applied in the **AP1000** safety case for SSCs that protect against internal and external hazards.
- The fault schedule and hazard schedules make a useful contribution to the PCSR, showing some of the expectations and properties set out in NS-TAST-GD-051 (Ref. 6) for a safety case.

89. There are some weaknesses in the fault schedule's treatment of non-reactor faults. While faults are listed, there is very limited visibility of the engineered SSCs that protect against faults not directly associated with the reactor or stop them from occurring. However, I have not judged this shortfall to be an impediment to closing the GDA Issue because large portions of the non-reactor safety case have been excluded from the scope of GDA. There is clear expectation that areas of the safety case out of scope of GDA will need to be addressed during site licensing, and the fault schedule (as a 'live' aspect of the PCSR) will need to be updated to reflect the work done to complete the scope of the safety case. Therefore, I have not identified the need for any specific Assessment Findings for a future licensee to address that are in addition to 'normal business' of producing an adequate safety case to facilitate operations of a new nuclear power plant.

90. Ultimately, I am satisfied that GDA Issue GI-AP1000-FS-08 can be closed.

6 REFERENCES

1.	Step 4 Fault Studies – Design Basis Faults Assessment of the Westinghouse **AP1000** Reactor, ONR-GDA-AR-11-004a Revision 0, November 2011, TRIM Ref. 2010/581406.
2.	**AP1000** Pre-Construction Safety Report, UKP-GW-GL-793 Revision 0, March 2011, TRIM Ref. 2011/192251.
3.	UK **AP1000** Assessment Plan for Closure GDA Fault Studies Issues 1 to 8, ONR-GDA-AP-14-002 Revision 0, March 2015, TRIM Ref. 2015/51535.
4.	ONR Guidance on Mechanics of Assessment, TRIM Ref. 2013/204124.
5.	GDA Guidance to Requesting Parties. www.onr.org.uk/new-reactors/ngn03.pdf
6	The Purpose, Scope, and Content of Safety Cases, NS-TAST-GD-051 Revision 4. www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-051.pdf
7.	GDA Issue “PCSR to Support GDA”, GI-AP1000-CC-02 Revision 3. www.onr.org.uk/new-reactors/reports/step-four/westinghouse-gda-issues/gi-ap1000-cc-02.pdf
8.	Purpose and Scope of Permissioning, NS-PER-GD-014 Revision 5, TRIM Ref. 2015/304735.
9.	Safety Assessment Principles for Nuclear Facilities. 2014 Edition Revision 0, ONR, November 2014. www.onr.org.uk/saps/saps2014.pdf
10.	IAEA Standards and Guidance: International Atomic Energy Agency (IAEA) Safety Standards Series – Safety of Nuclear Power Plants: Design, Specific Safety Requirements (SSR) 2/1, Revision 1, 2016. www.iaea.org.
11.	Response to RO-AP1000-46 and RO-AP1000-46.A1.1 – List of Design Basis Initiating Events Following ND Comments on the Westinghouse Response of 28 May 2010, Unique Number REG Westinghouse 000290, Letter from **AP1000** Project Front Office to ND, 10 August 2010, TRIM Ref. 2010/351527
12.	**AP1000** Pre-Construction Safety Report, UKP-GW-GL-793 Revision 1, January 2017, TRIM Ref. 2017/43700.
13.	Step 4 Control and Instrumentation Assessment of the Westinghouse **AP1000** Reactor, ONR-GDA-AR-11-006 Revision 0, November 2011, TRIM Ref. 2010/581525.
14.	Response to Regulatory Query “Review of the Fault Schedule against PCSR Chapter 9 (FS-08)”, RQ-AP1000-1788, TRIM Ref. 2017/22506.
15.	**AP1000®** UK Generic Technical Specifications, UKP-GW-GL-501 Revision 0, January 2016, TRIM Ref. 2016/40641.
16.	Recommendation for Development of the **AP1000** Technical Requirements Manual, UKP-GW-GL-502 Revision 0, February 2016, TRIM Ref. 2016/54147