Office for Nuclear Regulation

An agency of HSE

Generic Design Assessment – New Civil Reactor Build

GDA Close-out for the EDF and AREVA UK EPR™ Reactor
GDA Issue GI-UKEPR-IH-03 Revision 2 – Internal Flooding Safety Case

Assessment Report: ONR-GDA-AR-12-018
Revision 0A
January 2013

COPYRIGHT

First published January 2013

EXECUTIVE SUMMARY

This report presents the close-out of the Office for Nuclear Regulation's (ONR), an agency of the Health and Safety Executive (HSE), Generic Design Assessment (GDA) for the GDA Issue GI-UKEPR-IH-03 Revision 2 and the associated GDA Issue Action generated as a result of the GDA Step 4 Internal Hazards Assessment of the UK EPR™. The assessment has focussed on the deliverables identified within the EDF and AREVA Resolution Plans published in response to the GDA Issue and on further assessment undertaken of those deliverables.

During Step 4 it became apparent that the internal flooding claims stated within the PCSR were inconsistent with the deterministic approach to the analysis of potential sources of internal flooding. As a result, substantiation was required of the internal flooding safety case through a deterministic analysis that initially assumed an unmitigated flood source and applied a multi-legged argument.

In response to the GDA Issue, EDF and AREVA provided a Resolution Plan that committed to providing a dedicated internal flooding safety case based upon a deterministic analysis that assumed an unmitigated flood source. The Resolution Plan split the analysis into two separate tasks. The first task was to undertake an analysis considering the main flooding initiators in each safety classified building of the Nuclear Island with the assumption that the flood was not mitigated by a manual action. Further to the identification of the flooding initiators, each bounding leak volume was then compared to the water volume for which the particular safety classified building had been sized.

If the flooding event demonstrated that there was insufficient water retention capacity within the affected building, the consequences were considered as unacceptable as the event could threaten more than one redundant safety significant system. Task 2 then considered these specific scenarios and provided further detailed mitigation that considered the following additional ALARP measures:

- Enhancement of the hazard barriers.
- Further engineered solutions e.g. automatic means by which to isolate potential sources of internal flooding.
- Consideration of operator actions including the viability of the potential action to be undertaken.

A further deliverable was submitted as a result of the assessment of the first two submissions as the approach taken was inconsistent with my expectations due to the assumption of leak rather than complete break for classified moderate energy pipework with a nominal diameter greater than 50mm. This further deliverable presented multi-legged arguments and an ALARP consequence analysis associated with internal flooding which considered such breaks in moderate energy pipework.

EDF and AREVA identified the following systems gross failure of which could lead to an internal flooding event with the potential to affect more than one redundant safety significant system:

- Fire fighting system within the Annulus
- Essential service water system within the Safeguards Auxiliary Buildings
- Demineralised water system within the Annulus

As a result, EDF and AREVA identified three design changes associated with these systems.

The first relates to changing seven manual valves to motorised ones that can be operated automatically in the event of sump level detection and operation of the classified fire fighting water

supply system (JAC) pumps. In addition, a further four motorised valves have been added to take into account single failure. The additional electrical and control and instrumentation (C&I) has also been identified for both the change from manual to motorised valves and for the new motorised valves. Finally, a two step isolation signal for the hose reels and sprinkler system within the Annulus has been introduced to automatically isolate the system 20 minutes after flood detection by the sump level measurement. This isolation will mean that flood levels do not result in loss of more than one redundant safety significant system. In addition, the automatic isolation after 20 minutes ensures that the automatic fire fighting system (sprinkler system) is operational for a sufficient period to support the fire fighting strategy in case of "internal flooding" spurious signal.

The second modification relates to additional flood level detection and preventative pump trip of the Essential Service Water System (ESWS) within the Safeguard Auxiliary Buildings. Sensors are to be placed [redacted] above the floor at the [redacted] level in each of the SABs to ensure that should failure of the ESWS occur, then there is sufficient time and relevant information for operators to realign the ESWS onto a different division and to isolate the affected ESWS in advance of water reaching the [redacted] level.

The final modification relates to improved isolation of the Demineralised Water System (SED) within the annulus. This is achieved by a change from a manual valve to one that is motorised. There are also changes to the operational procedures associated with preventive isolation in the event of detection of flooding within the Annulus.

The change management forms (CMF) recognise that the modifications require categorisation to be undertaken during the Site Specific Phase.

I am content with the design changes proposed for UK EPR™ and believe that such changes will result in a far more robust safety case in the event of gross failure of systems contained within the Safeguard Auxiliary Buildings and Reactor Building Annulus.

There have been three Assessment Findings raised as a result of this assessment.

The totality of the deliverables submitted provides a comprehensive analysis of potential sources of internal flooding within the UK EPR™ and together with the flooding analyses completed for FA3 which demonstrate the detailed approach to the analysis of drainage and discharge routes, I am satisfied that the safety case for internal flooding is robust. The submissions address the range of potential failure mechanisms, consider the barriers and doors in place to prevent flood propagation affecting more than one redundancy, and include both engineered and administrative measures to mitigate potential flooding events. As a result the analysis has identified reasonably practicable modifications which result in improvements in the robustness of the internal flooding safety case. I have reviewed the final GDA PCSR and am content that it reflects the additional analysis work that has been undertaken in support of the UK EPR™

I am, therefore, satisfied that GDA Issue, GI-UKEPR-IH-03, can now be closed.

LIST OF ABBREVIATIONS

ALARP	As low as is reasonably practicable
AREVA	AREVA NP SAS
AVS	Annulus Ventilation System
C&I	Control and Instrumentation
CCWS	Component Cooling Water System
CHRS	Containment Heat Removal System
CMF	Change Management Form
CSBVS	Controlled Safeguard Building Ventilation System
DB	Diesel Building
DEGB	Double Ended Guillotine Break
EDF	Electricité de France SA
EFWS	Emergency Feedwater System
ESWS	Essential Service Water System
FA3	Flamanville 3 Nuclear Power Plant
FB	Fuel Building
FPCS	Fuel Pool Cooling System
GDA	Generic Design Assessment
HDA	Diesel Building A
HDB	Diesel Building B
HRA	Reactor Building Containment
HRB	Reactor Building Annulus
HSE	Health and Safety Executive
HVAC	Heating Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
IRWST	In-containment Refuelling Water Storage Tank
JAC	Classified Fire Fighting Water Supply System
JPI	Nuclear Island Fire Protection System
JPV	Diesel Buildings Protection and Fire Fighting Distribution System
MCR	Main Control Room
NAB	Nuclear Auxiliary Building
ND	Nominal Diameter
NI	Nuclear Island

LIST OF ABBREVIATIONS

NVDS	Nuclear Island Vent and Drain System
OL3	Olkiluoto 3 Nuclear Power Plant
ONR	Office for Nuclear Regulation (an agency of HSE)
PCC	Plant Condition Category
PCSR	Pre-construction Safety Report
RB	Reactor Building
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
SAB	Safeguard Auxiliary Building
SAP	HSE Safety Assessment Principles
SBO	Station Black-Out
SED	Demineralised Water Distribution System
SEP	Drinking Water System
SER	Demineralised Water Distribution pH9 System
SSCs	Systems, Structures and Components
TAG	Technical Assessment Guide(s) (ONR)
TQ	Technical Query
UCWS	Ultimate Cooling Water System

TABLE OF CONTENTS

Tables

Annexes

1 INTRODUCTION

1.1 Background

1 This report presents the close-out of the Office for Nuclear Regulation's (ONR), an agency of the Health and Safety Executive (HSE), Generic Design Assessment (GDA) for the GDA Issue GI-UKEPR-IH-03 Revision 2 and the associated GDA Issue Action (Ref. 5) generated as a result of the GDA Step 4 Internal Hazards Assessment of the UK EPR™ (Ref. 6). The assessment has focussed on the deliverables identified within the EDF and AREVA Resolution Plan (Ref. 7) published in response to the GDA Issue and on further assessment undertaken of those deliverables.

2 GDA followed a step-wise-approach in a claims-argument-evidence hierarchy. In Step 2 the claims made by the EDF and AREVA were examined and in Step 3 the arguments that underpin those claims were examined. The Step 4 assessment reviewed the safety aspects of the UK EPR™ reactor in greater detail, by examining the evidence, supporting the claims and arguments made in the safety documentation.

3 The Step 4 Internal Hazards Assessment identified four GDA Issues and a number of Assessment Findings as part of the assessment of the evidence associated with the UK EPR™ reactor design. GDA Issues are unresolved issues considered by regulators to be significant, but resolvable, and which require resolution before nuclear island safety related construction of such a reactor could be considered. Assessment Findings are findings that are identified during the regulators' GDA assessment that are important to safety, but not considered critical to the decision to start nuclear island safety related construction of such a reactor.

4 The Step 4 Assessment concluded that the UK EPR™ reactor was suitable for construction in the UK subject to resolution of 31 GDA Issues. The purpose of this report is to provide the assessment which underpins the judgement made in closing GDA Issue GI-UKEPR-IH-03.

1.2 Scope

5 This report presents only 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 Internal Hazards Assessment of the EDF and AREVA UK EPR™ (Ref. 6) in order to appreciate the totality of the assessment of the evidence undertaken as part of the GDA process.

6 This assessment report is not intended to revisit aspects of assessment already undertaken and confirmed as being adequate during previous stages of the GDA. However, should evidence from the assessment of EDF and AREVA's responses to GDA Issue highlight shortfalls not previously identified during Step 4, there will be a need for these aspects of the assessment to be highlighted and addressed as part of the close-out phase or be identified as Assessment Findings to be taken forward to Site Specific Phase.

7 The possibility of further Assessment Findings being generated as a result of this assessment is not precluded given that resolution of the GDA Issue may leave aspects of the assessment requiring further detailed evidence when the information becomes available at a later stage.

8 During Step 4 it became apparent that the internal flooding claims stated within the PCSR were inconsistent with the deterministic approach to the analysis of potential sources of internal flooding. As a result the GDA Issue, GI-UKEPR-IH-03, was raised, which required EDF and AREVA to produce a safety case that involved undertaking a

deterministic analysis. The analysis was to initally assume an unmitigated flood source and then apply a multi-legged argument that considered the array of measures in place to mitigate potential flooding events including civil engineering design and engineered and administrative controls.

1.3 Methodology

9 The methodology applied to this assessment is identical to the approach taken during Step 4 which followed the ONR HOW2 document PI/FWD, *"Permissioning – Purpose and Scope of Permissioning"* (Ref. 1), in relation to mechanics of assessment within ONR.

10 This assessment has been focused primarily on the submissions relating to resolution of the GDA Issue as well as any further requests for information or justification derived from assessment of those specific deliverables.

11 The assessment allows ONR to judge whether the submissions provided in response to the GDA Issue are sufficient to allow it to be closed. Where requirements for more detailed evidence have been identified that are appropriate to be provided at the design, construction or commissioning phases of the project these can be carried forward as Assessment Findings.

1.4 Structure

12 This Assessment Report structure differs slightly from the structure adopted for the previous reports produced within GDA, most notably the Step 4 Internal Hazards Assessment. The report has been structured to reflect the assessment of the individual GDA Issue rather than a report detailing close-out of all GDA Issues associated with this technical area.

13 The reasoning behind adopting this report structure is to allow closure of GDA Issues as the work is completed rather than having to wait for the completion of all the GDA work in this technical area.

2 ONR'S ASSESSMENT STRATEGY FOR INTERNAL HAZARDS

14 The intended assessment strategy for GDA Close-out for the internal hazards topic area was set out in an Assessment Plan (Ref. 11) that identified the intended scope of the assessment and the standards and criteria that would be applied.

15 The overall bases for the assessment of the GDA Issue are the internal hazards elements of:

- Submissions made to ONR in accordance with the resolution plans.
- Update to the Submission / Pre-construction Safety Report (PCSR) / Supporting Documentation.
- The Design Reference that relates to the Submission / PCSR as set out in UK EPR™ GDA Project Instruction UKEPR-I-002 (Ref. 8) which will be updated throughout GDA Issue resolution and includes any Change Management Forms (CMF).
- Design Change Submissions – which are proposed by EDF and AREVA and submitted in accordance with UK EPR™ GDA Project Instruction UKEPR-I-003 (Ref. 9).

2.1 The Approach to Assessment for GDA Close-out

16 The approach to the closure of this GDA Issue for the UK EPR™ Project involves:

- Assessment of submissions made by EDF and AREVA in response to the GDA Issue identified through the GDA process. These submissions are detailed within the EDF and AREVA Resolution Plan for the GDA Issue.
- In the event of requiring further supporting evidence for the assessment, Technical Queries (TQ) (Ref. 13) have been generated.
- When requests for further information through production of the aforementioned TQs did not adequately resolve the GDA Issue, formal notification in the form of a letter detailing the shortfall(s) in ONR expectations was sent to EDF and AREVA.

17 If the assessment of the submissions together with any design changes requested by EDF and AREVA are judged acceptable, the GDA Issue can be cleared.

2.2 Standards and Criteria

18 The relevant standards and criteria adopted within this assessment are principally the Safety Assessment Principles (SAPs) (Ref. 2), internal ONR Technical Assessment Guides (TAG) (Ref. 3), relevant national and international standards, and relevant good practice informed from existing practices adopted on UK nuclear licensed sites. The key SAPs and relevant TAGs have been detailed within this section. National and international standards and guidance have been referenced where appropriate within the assessment report. Relevant good practice, where applicable, has also been cited within the body of the assessment.

2.2.1 Safety Assessment Principles

19 The key SAPs (Ref. 2) applied within the Internal Hazards Assessment of the EDF and AREVA UK EPR™ are included within Table 1 of this report.

2.2.2 Technical Assessment Guides

20 The following Technical Assessment Guides have been used as part of this assessment (Ref. 3):

- T/AST/006 Issue 03 – Deterministic Safety Analysis and the Use of Engineering Principles in Safety Assessment
- T/AST/010 Issue 02 – Early Initiation of Safety Systems.
- T/AST/014 Issue 02 - Internal Hazards
- T/AST/017 Issue 02 – Structural Integrity Civil Engineering Aspects
- T/AST/036 Issue 02 – Diversity, Redundancy, Segregation and Layout of Mechanical Plant
- T/AST/051 Issue 01 – Guidance on the Purpose, Scope and Content of Nuclear Safety Cases

2.2.3 International Standards and Guidance

21 The following international standards and guidance have been used as part of this assessment:

- Safety of Nuclear Power Plants: Design. Safety Requirements, NS-R-1(Ref. 4)
- Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants. Safety Guide, NS-G-1.11 (Ref. 4)

2.3 Use of Technical Support Contractors

22 No Technical Support Contractors were utilised in the assessment of this GDA Issue.

2.4 Out-of-scope Items

23 As part of the GDA Closeout, no items have been identified as being out of scope by EDF and AREVA as a result of this assessment.

3 EDF AND AREVA DELIVERABLES IN RESPONSE TO THE GDA ISSUE

24 The GDA Issue, GI-UKEPR-IH-03, was raised as the internal flooding claims stated within the PCSR were inconsistent with the deterministic approach to the analysis of potential sources of internal flooding. As a result the action required EDF and AREVA to provide adequate substantiation of internal flooding through the production of a deterministic multi-legged safety case that assumed an unmitigated flood source. The GDA Issue Action suggested that EDF and AREVA may wish to consider the following in the production of such a case:

- Potential failure mechanisms of water based systems.
- Civil engineering aspects including barriers and drainage.
- Systems (both engineered and administrative) to ensure that the effects of an internal flooding event are limited to loss of one division.
- Any further defence in depth and ALARP measures that could be implemented into the design.
- The impact of the changes made to the PCSR relating to the outcome of this substantiation on other safety case submissions such as civil engineering and human factors.

25 In response to the GDA Issue, EDF and AREVA provided a Resolution Plan (Ref. 7) detailing how they intended to address the above points. The Resolution Plan stated that a dedicated internal flooding safety case based upon a deterministic analysis that assumes an unmitigated flood source would be provided.

26 The Resolution Plan split the analysis into two separate tasks. The first task was to undertake an analysis considering the main flooding initiators in each safety classified building of the Nuclear Island (NI) with the assumption that the flood was not mitigated by a manual action. Further to the identification of the flooding initiators, each bounding leak volume was then compared to the water volume for which the particular safety classified building had been sized.

27 If the flooding event demonstrated that the volume of water retention of the affected building is not sufficient, then the consequences will be considered as unacceptable as the event could threaten more than one redundant safety significant system. Should this be the case, then Task 2 would consider these specific scenarios with a view to providing sufficient detail mitigation culminating in an ALARP study that would consider the following additional measures:

- Enhancement of the hazard barriers.
- Further engineered solutions e.g. automatic means by which to isolate potential sources of internal flooding.
- Consideration of operator actions including the viability of the potential action to be undertaken.

28 A further deliverable was submitted as a result of the assessment of the first two deliverables. The deliverable presented multi-legged arguments and an ALARP consequence analysis associated with internal flooding which considered breaks in classified moderate energy pipework with a nominal diameter greater than 50mm.

29 The information provided by EDF and AREVA in response to this GDA Issue was broken down into the following specific deliverables for detailed assessment:

GDA Issue Action	Internal Hazard	Deliverable	Ref.
GI-UKEPR-IH-03.A1	Internal Flooding	Internal Flooding – Identification of bounding cases: leak volumes and retention volumes	14
GI-UKEPR-IH-03.A1	Internal Flooding	Internal Flooding - Bounding cases: mitigation measures	15
GI-UKEPR-IH-03.A1	Internal Flooding	UK EPR™ - Internal Flooding – Multi-legged safety case and ALARP consequence assessment analysis.	16

30 An overview of each of the deliverables is provided within this section. It is important to note that this information is supplementary to the information provided within the March 2011 Consolidated PCSR (Ref. 10) which has already been subject to assessment during earlier stages of GDA.

31 It is important to recognise the deliverables associated with this GDA Issue use the existing French approach to classification and categorisation of Structures, Systems, and Components (SSCs). The use of categorisation and classification is addressed as part of the work undertaken in response to the cross cutting GDA Issue, GI-UKEPR-CC-01. As a result, EDF and AREVA identify four types of safety functions; F1A, F1B, F2 and Non-Classified (NC). An F1A safety function is a function that is required for a Plant Condition Category (PCC) event to reach the controlled state. An F1B safety function is a function that is required to reach the safe shutdown state. F2 safety functions are claimed for Risk Reduction Category (RRC), RRC-A and RRC-B sequences.

3.1 Internal Flooding – Identification of bounding cases: leak volumes and retention volumes, ECEIG110718 Revision A

32 The above submission (Ref. 14) identifies the bounding cases for potential internal flooding events within the nuclear island buildings. The approach taken involves calculating the maximum retention volumes for each NI building assuming that the interface and peripheral barriers are designed to withstand a [redacted] water column. This design feature results in all such barriers beneath the [redacted] level being designed to be water tight. In addition, the volumes calculated for each building take into account a [redacted] reduction to allow for equipment installed within the area.

33 The next step of the process is to identify the maximum flooding volume generated as a result of failure of fluid carrying systems. Each fluid retaining system has been subject to analysis to determine the maximum potential volume that could be released as a result of failure of that system. The volume released assumes loss of the entire contents of the system as well as any make-up systems in place if automatically initiated.

34 The final step in the process is to consider the impact of the flooding scenarios identified. It is assumed that any water released would flow into floor drains, down staircases, and through unclosed openings to the lowest levels of the building and each bounding leak is compared with the relevant retention volume of the building in question. The outcome of the analysis then identifies two potential outcomes:

- If the system's maximum released volume is contained within the water retention volume for the building in question, then no further studies are undertaken;

- If the system's maximum released volume exceeds the water retention volume, a calculation of the released flow rate is performed in order to establish the time it would take for the water to reach the [redacted] level.

35 When considering the leak rates from failed pipework, the analysis conservatively assumes that there are no head losses and that the pressure inside the failed pipe remains unchanged. In addition, there was an assumption that moderate energy pipework of a pressure retaining component quality (Q3 quality as defined within the Flamanville 3 project) and with a nominal diameter (ND) >50mm only leaked with a leak size equivalent to the nominal diameter multiplied by the pipe thickness divided by four (Dt/4). Please note that this claim has since been supplemented by further ALARP arguments detailed within Reference 16.

36 The following buildings are then subject to detailed analysis adopting the above principles:

- Reactor Building Containment (HRA) and Annulus (HRB)
- Fuel Building (FB)
- Safeguard Auxiliary Buildings (SAB)
- Diesel Buildings (DB)
- Nuclear Auxiliary Building (NAB)

37 Each of the potential internal flooding volumes has been subject to analysis for each of the buildings above with a summary of the conclusions presented below.

38 The outcome of the analysis is then included as part of the further submission (Ref. 15) associated with the identification of mitigation measures. It is important to note that mitigation in the form of operator actions are not fully captured within this Reference 14 as these have been captured within Reference 22; however, reference is made to detection and alarm, where applicable.

3.1.1 Reactor Building Containment and Annulus

39 The Containment (HRA) and Annulus (HRB) have volumes of [redacted] and [redacted] respectively. The Containment is not specifically sized to withstand internal flooding events, however, the structure is designed to withstand an overpressure of [redacted] as part of the severe accident analysis. As a result, the Containment is sufficient to withstand the effects of a volume of water with an equivalent head of pressure of [redacted].

3.1.1.1 Detection and Alarm

40 The analysis for the Containment considers the path that water would take in the event of an internal flooding event. In the majority of flooding events the water would flow to the In-containment Refuelling Water Storage Tank (IRWST). The IRWST contains a large quantity of borated water and acts as a retention volume for flooding events. There are [redacted] redundant F1B level sensors located within the IRWST that would detect any additional water at the "MAX1", the location of the level sensor at the [redacted] level. Actuation of the redundant level sensors would result in an alarm being raised within the Main Control Room (MCR), however, this would not identify the specific source of the flood water.

41 In the event of a flooding event within the Annulus, any flood water would flow into the Nuclear Island Vent and Drain System (NVDS) sump at the [redacted] level and would alarm in the MCR, however, this would not identify the specific source of the flood water.

3.1.1.2 Flooding Initiators

42 Each of the water containing systems contained within both the Containment and Annulus are analysed to determine the maximum amount of water that would be released as a result of failure and it is ascertained whether failure of the system constitutes a *major flood initiator*. The major flood initiators are identified as those that have an unlimited upstream volume. There is consideration of both manual and automatic isolation as a result of failure of the systems as well consideration of the times taken for flood levels to reach MAX1 [redacted] level) in the IRWST. When the time to automatic isolation cannot be determined, then conservative assumptions associated with water volumes arising from upstream tanks are applied.

43 The following systems have been identified as major flood initiators within the Containment:

- Demineralised Water System (SED).
- Component Cooling Water System (CCWS).

44 The water volumes assumed in the analysis apply an approach that only considers leaks in moderate energy systems with an ND>50mm, namely, the nuclear island fire protection system (JPI). The size of the leak in these cases is calculated to be the pipework diameter multiplied by the wall thickness, divided by four (Dt/4). In addition, break preclusion arguments are claimed in the event of failure of the Fuel Pool Cooling System (FPCS).

45 The following systems have been identified as major flood initiators within the Annulus:

- Demineralised Water System (SED).
- Nuclear Island Fire Protection System (JPI).

46 As was the case for the Containment, Dt/4 leaks with an ND>50mm are assumed in the moderate energy systems.

3.1.1.3 Flooding Analysis

47 Each of the systems identified as major flooding initiators are considered further within the detailed analysis.

48 The flooding scenario associated with failure of the SED within Containment would be caused by a break in an ND50 pipe and would result in break flow rate of [redacted]. This flow rate would result in the IRWST overflowing after 35 minutes. In order to terminate the flooding event, the F1A classified motorised valves, [redacted] or the manual valve, [redacted] would need to be closed. As the SED is not a safety classified system the design makes no provision by which to detect the flooding event other than the level monitoring within the IRWST when it reaches MAX1. As explained earlier, the level monitoring would not be able to identify the source of flooding, and it is proposed that a preventative isolation of the SED would be undertaken noting that the isolation would have no detrimental impact on nuclear safety.

49 The failure of the CCWS within Containment involves the consideration of leaks from pipework with a flow less than [redacted] as any flow greater than this would result in the automatic isolation of the CCWS and subsequent halting of the make-up from the

SED. The only section of pipework that could result in a flow less than [redacted] would involve a Dt/4 leak in the ND100 pipework. In this scenario it would take 12 hours for the leak to reach the [redacted] level and as no CCWS alarm is activated, the MAX1 level alarms within the IRWST would notify operators within the MCR of the flooding event. Again, the source of the flooding would not be known to operators. This scenario is therefore bounded by the flooding event associated with failure of the SED system, detailed previously, albeit the mitigation actions would be different given that isolation of the CCWS could have potential safety consequences.

50 The flooding event associated with the JPI system within the Annulus considers guillotine failure of an ND50 diameter pipe. The resultant flow from the JPI system, based on the nominal operating pressures of [redacted], is calculated to be [redacted] assuming no head losses from the system. The capacity of the JPI tank is [redacted] and, assuming the tank empties at a constant flow rate, results in the level in the Annulus being [redacted] above the [redacted] level after a period of 7 hours assuming that there is no mitigation action taken by operators. Once the initial content of the tanks has been lost then water would continue to flow from the JPI system, but at a rate equivalent to the make-up rate of the tank ([redacted]) assuming that no action has been taken to terminate the flood.

51 A ND50 break in the SED within the Annulus would take 4 hours to reach a water column height of 3.5m at the [redacted] level given a flow rate of [redacted] from the [redacted] storage tank.

3.1.1.4 Conclusions

52 The submission concludes that the SED and CCWS systems are the only major flooding initiators in Reactor Building Containment, and in all cases the detection is performed by the level increase in the IRWST. A preventive isolation of the SED is required if the level MAX1 is reached in the IRWST.

The major flooding initiators in the Reactor Building Annulus are the JPI and SED systems.

3.1.2 Fuel Building

53 The Fuel Building (FB) is separated into two divisions; Division 1 and Division 4 with the barrier between the two divisions being watertight up to the [redacted] level. The retention volumes of the two divisions beneath the [redacted] level are [redacted] and [redacted], respectively. The barrier segregating to the two divisions is claimed to be watertight up to the [redacted] level, hence the capacity of the retention volumes.

3.1.2.1 Detection and Alarm

54 As is the case for the Reactor Building Annulus, there is an NVDS sump that would detect that water was present and relay the information back to the MCR, however, it would not be possible to identify the specific source of the flooding initiator.

3.1.2.2 Flooding Initiators

55 As was the case for the Reactor Building, each of the potential flooding initiators has been analysed to determine whether there are any major flooding initiators that require further analysis.

56 The following systems have been identified as major flood initiators within the Fuel Building:

- Nuclear Island Fire Protection System (JPI).
- Component Cooling Water System (CCWS).
- Demineralised Water System (SED).

57 All other systems reviewed have a limited upstream volume and the volume of water can be contained in the basement levels of the Fuel Building.

3.1.2.3 Flooding Analysis

58 Each of the systems identified as major flooding initiators are considered further within the detailed analysis.

59 The flooding scenario associated with the failure of the JPI system identifies that in the event of a guillotine break of an ND50 pipe it would take 10 and 12 hours to reach the [redacted] level in Divisions 1 and 4 respectively. This calculation is based on a flow rate of [redacted] initially, resulting in complete drainage of the [redacted] tank followed by the additional flow of [redacted] associated with the make-up rate of the tank. This calculation assumes that the leak is neither detected nor is it isolated and does not consider head losses associated with the pipework.

60 A leak in a ND100 pipe has been identified as the most onerous flooding scenario associated with the CCWS in the Fuel Building. This is the maximum failure at which the flow would be less than [redacted] given that any flow greater than this would result in the automatic isolation of the SED. The time that it would take for the resultant leak to reach the [redacted] level within Divisions 1 and 4 would be 255 and 280 hours respectively, assuming that it is neither detected nor isolated. The submission states that this flooding scenario is bounded by the failure associated with the SED.

61 The worst failure of the SED within the Fuel Building is a failure of an ND50 diameter pipe within the SED 4 system which results in a flow of [redacted] emptying the [redacted] tank in the first instance, then followed by a flow of [redacted] from the make-up to the tank. The time to reach the [redacted] level is calculated to be 20 and 22 hours for Division 1 and 4 respectively.

3.1.2.4 Conclusions

62 The submission concludes that maximum released volume on almost all systems can be contained in one division basement level. Only the JPI, CCWS, and the SED systems are significant flooding initiators that could reach the [redacted] level if no operator action were taken to mitigate the flooding.

63 For the SED system, the worst scenario is a break of an ND25 pipe in Division 4. The report states, *"Using the maximum calculated released flow rate, it would take between 25 and 27 hours for the water to reach level* [redacted] *in one division"*.

64 In the case of the JPI system there are several flooding scenarios in Fuel Building due to the pipes of differing diameters. The submission concludes that the worst flooding scenario is a ND50 pipe break and states, *"Using the maximum calculated released flow rate, it would take between 15 and 17 hours for water to reach level* [redacted] *in one division."*

65 It is stated that the flooding durations have been estimated with the assumption of no head losses through the system from the storage tank to the leak location. As a result the report concludes that the timescales were pessimistic given the conservatism applied in the flow rates for the scenarios analysed.

3.1.3 Safeguard Auxiliary Buildings

66 There are four Safeguard Auxiliary Buildings (SABs) located around the Reactor Building which have divisional segregation. Each divisional building is further segregated into a mechanical and electrical division. The mechanical division is located at the [redacted] level and below and the electrical division located above the [redacted] level. The levels beneath the [redacted] level are utilised as retention volumes for each of the buildings and the barriers beneath this level are claimed as flood barriers resistant to a [redacted] water column. The retention volumes for each of the SABs is shown below:

Level	SAB 1 Volume (m^3)	SAB 2 Volume (m^3)	SAB 3 Volume (m^3)	SAB 4 Volume (m^3)
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Total Retention Volume	[redacted]	[redacted]	[redacted]	[redacted]

3.1.3.1 Detection and Alarm

67 As with the other nuclear island buildings studied, there are NVDS sumps installed in each SAB which would detect that water was present and relay the information back to the MCR, however, it would not be possible to identify the specific source of the flooding initiator.

3.1.3.2 Flooding Initiators

68 Each of the systems identified as major flooding initiators are considered further within the detailed analysis.

69 The following systems have been identified as major flood initiators within the Safeguard Auxiliary Buildings:

- Nuclear Island Fire Protection System (JPI).
- Component Cooling Water System (CCWS).
- Essential Service Water System (ESWS)
- Demineralised Water System (SED).
- Drinking Water Distribution System (SEP)
- Demineralised Water Distribution pH9 System (SER) feed to the EFWS in SAB 4
- Ultimate Cooling Water System (UCWS) feed to the Containment Heat Removal System (CHRS) in SAB 1 and SAB 4.

70 The above systems are considered as major flooding initiators given that the upstream water volumes are unlimited if actions are not taken to mitigate the flooding consequences.

71 The maximum released volumes for the other systems analysed are contained within the water retention volumes for the respective SAB.

3.1.3.3 Flooding Analysis

72 Each of the systems identified as major flooding initiators are considered further within the detailed analysis. The flow rates together with the timescales for the worst major flooding initiators for each SAB are shown below:

System	Failure (Break or Leak)	Nominal Diameter (mm)	Flowrate (m^3/h)	Time to Level [redacted] (hours)		
				SAB 1	SABs 2 & 3	SAB 4
JPI	Break	50	[redacted]	21	18	20
CCWS	Leak	80	[redacted]	515	-	503
CCWS	Leak	100	[redacted]	-	355	-
ESWS	Leak	700	[redacted]	21	19	20
SED	Break	50	[redacted]	34	29	31
SEP	Break	50	[redacted]	19	17	18
SER	Break	25	[redacted]	-	-	56
UCWS	Leak	300	[redacted]	69	-	67

3.1.3.4 Conclusions

73 The submission concludes that the maximum released water volumes in the SAB are due to the following systems:

- JPI, CCWS (fed from the SED), SED, SEP, and ESWS with each system contained within each of the four SAB.
- UCWS in SAB1 and SAB4 (feed to the CHRS)
- SER in SAB 4 (feed to the EFWS).

74 For each of the above systems, their upstream volume could be unlimited if no manual actions are performed to mitigate the flooding event.

75 For the other systems analysed the maximum released volumes of the other systems are either contained in the retention volume of the SAB division or initiate PCC events detailed within the March 2011 Consolidated PCSR (Ref. 10).

76 The most significant flooding initiators identified within the submission for all SAB are an ND50 pipe break in the JPI or SEP or a leak in an ND700 pipe associated with the ESWS. For each of the scenarios identified there is approximately 20 hours in which for the break/leak to detected and isolated. As stated previously, if head losses were taken into account the durations for detection and isolation would be longer.

3.1.4 Diesel Buildings

77 There are two Diesel Buildings (DB) geographically separated whose design is identical. Each building contains two diesel sets (Divisions 1 and 2 or Divisions 3 and 4) and one Station Blackout (SBO) diesel. As was the case for the SABs the levels beneath [redacted] in each of the diesel buildings are designed as retention volumes for flooding.

There are watertight barriers between each of the diesel sets including the SBO diesels that are qualified to withstand a water column height of [redacted]. The retention volumes for each of the two sections of the building containing the diesel sets are [redacted] with the retention volume of the section of the building containing the SBO diesel being [redacted].

3.1.4.1 Detection and Alarm

78 As with the other nuclear island buildings studied, there are NVDS sumps installed in the Diesel Buildings, which would detect that water was present and relay the information back to the MCR, however, it would not be possible to identify the specific source of the flooding initiator.

3.1.4.2 Flooding Initiators

79 Each of the potential flooding initiators have been analysed for each of the DBs to determine whether they are any major flooding initiators that require further analysis.

80 The following systems have been identified as major flood initiators within the DBs:

- Diesel Buildings Protection and Fire Fighting Distribution System (JPV).
- Demineralised Water System (SED).
- Drinking Water System (SEP).

81 The above systems are major flooding initiators as their upstream volumes could exceed the water retention volume if the leak or break is not mitigated.

82 The other systems analysed are shown to contain insufficient quantities of water to result in the retention volume being exceeded.

3.1.4.3 Flooding Analysis

83 Each of the systems identified as major flooding initiators are considered further within the detailed analysis.

84 The flow rates together with the timescales for the worst major flooding initiators for the DBs are shown below:

System	Failure (Break or Leak)	Nominal Diameter (mm)	Flowrate (m^3/h)	Time to Level [redacted] (hours)	
				SBO	Divisional Diesels
JPV	Break	50	[redacted]	4	5
SED	Break	25	[redacted]	20	26
SEP	Break	25	[redacted]	21	27

3.1.4.4 Conclusions

85 The submission recognises that the building retention volumes for the Diesel Buildings are significantly smaller than other nuclear island buildings, however, the potential flood initiators are fewer. Failure of the SED and SEP systems in a worst case scenario would allow at least 20 hours for detection and isolation.

86 The worst flooding scenario for the JPV results in 4 hours for the SBO and 5 hours for the divisional diesel buildings. The submission identifies that the calculations do not take into account head losses and therefore, the actual time for flood water to exceed the retention volume would be longer.

3.1.5 Nuclear Auxiliary Building

87 The Nuclear Auxiliary Building (NAB) is located adjacent to SAB 4 and the FB and has no classified F1 functions contained therein. There are three levels below [redacted] level that act as a retention volume for any potential flooding scenario with an approximate retention volume of [redacted].

3.1.5.1 Detection and Alarm

88 As with the other nuclear island buildings studied, there are NVDS sumps installed in the NAB, which would detect that water was present and relay the information back to the MCR, however, it would not be possible to identify the specific source of the flooding initiator.

3.1.5.2 Flooding Initiators

89 Each of the potential flooding initiators have been analysed for the Nuclear Auxiliary Building to determine whether they are any major flooding initiators that require further analysis.

90 The following systems have been identified as major flood initiators within the NAB:

- Nuclear Island Fire Protection System (JPI).
- Component Cooling Water System (CCWS).
- Demineralised Water System (SED).
- Drinking Water Distribution System (SEP)
- Demineralised Water Distribution pH9 System (SER) feed to the EFWS in SAB 4.

91 The above systems are major flooding initiators as their upstream volumes could exceed the water retention volume if the leak or break is not mitigated.

92 The other systems analysed are shown to contain insufficient quantities of water to result in the retention volume being exceeded.

3.1.5.3 Flooding Analysis

93 Each of the systems identified as major flooding initiators are considered further within the detailed analysis.

94 The flow rates together with the timescales for the worst major flooding initiators for the NAB are shown below:

System	Failure (Break or Leak)	Nominal Diameter (mm)	Flowrate (m^3/h)	Time to Level [redacted] (hours)
JPI	Break	50	[redacted]	40
CCWS	Leak	100	[redacted]	621
SED	Break	25	[redacted]	54

SEP	Break	50	[redacted]	30
SER	Leak	150	[redacted]	1065

3.1.5.4 Conclusions

95 The report concludes that the five systems identified could exceed the retention volume for the NAB, however, there would be at least 30 hours in which mitigation action could be taken.

3.1.6 Overall Conclusions

96 The submission concludes that the main flood initiators within the Nuclear Island buildings are the:

- Fire fighting systems, JPI and JPV both connected to the classified fire fighting water supply system (JAC) which is supplied by the SER.
- Small leaks in the Component Cooling Water System (CCWS) which is supplied by the SED.
- Demineralised water distribution systems, SED and SER.
- Drinking water distribution system (SEP)
- Essential Service Water System (ESWS) and the Ultimate Cooling Water System (UCWS)

97 The submission assumes an unlimited upstream volume of water as no mitigation actions are taken into account together with automatic water make-up provided from other upstream systems.

98 Further, the timescales in which to exceed the retention volumes in each case are relatively long given that there is no allowance for head losses in the pipework. The shortest duration being 4 hours in the case of break of ND50 JPI pipe within an SBO diesel building.

99 The other systems analysed demonstrate that they would not exceed the retention volume of the NAB building, however their failure may result in PCC transients which could require manual mitigation to manage, however, this is considered as part of the analysis of such transients within the PCSR.

100 Finally, it concludes that the mitigation measures will be considered within the submission, *"Internal Flooding – Bounding cases: mitigation measures"* (Ref. 15), an overview of which is provided within the next section of this assessment report.

3.2 Internal Flooding – Bounding cases: mitigation measures, ECEIG111647 Revision B

101 Further to the production of the report, *"Internal Flooding – Identification of bounding cases: leak volumes and retention volumes"* (Ref. 14), the above submission (Ref. 15) was provided as part of GDA to address those systems which have unlimited flood volumes and require detection and operator action to mitigate the flooding event.

102 The analysis considers further measures by which to reduce the risk to ALARP, namely:

- Design an engineering solution (e.g. automatic closure of a valve following flood detection).

- Enhance hazard barriers.
- Achieve an operator action (from the MCR or locally), considering the feasibility and risk associated with the action.

103 The submission considers the above ALARP measures from a qualitative approach and the buildings included within the scope are the:

- Reactor Building Containment (HRA) and Annulus (HRB).
- Fuel Building (FB).
- Safeguard Auxiliary Buildings (SAB).
- Diesel Buildings (DB).
- Nuclear Auxiliary Building (NAB).

104 The aim of the first step, an overview of which was detailed within Section 3.1 of this report, was to identify the shortfalls against the flooding barriers that provide segregation of safety significant structures, systems, and components (SSCs) in the event of internal flooding.

105 The second step, an overview of which is detailed within this section, is to consider those flooding events that could challenge the flood retention volumes as a result of the potentially unlimited flood sources that could arise as a result of a flooding initiator. Only the worst flooding scenario for each unmitigated flooding initiator is considered within this second step.

3.2.1 ALARP Assessment of the Options

106 Each of the three ALARP options are addressed in further detail within the submission, an overview of the basis of their application is provided within this section.

3.2.1.1 ALARP Option 1: Design an Engineering Solution

107 The submission identifies that priority should be given to the detection and automatic isolation of potential flooding initiators together with consideration of tripping of the associated pumps. The measures in place to undertake these actions should be safety classified and redundant in order to take into account the fact that mitigation means must be available as well as the single failure criterion. This option should also take into account the potential impact on nuclear safety of automatically isolating the system. Alternative engineered solutions are also identified associated with double piping sections of pipework e.g. high energy penetrations passing through the Annulus, and provision of dry pipework if the system is not required during normal plant operation.

3.2.1.2 ALARP Option 2: Enhance the Divisional Segregation Barriers

108 Whilst the existing divisional segregation barriers are qualified to withstand a [redacted] water column with the levels beneath the [redacted] level being capable of performing a water retention function, the further options of increasing the retention volume through increasing the height of the watertight barrier either by civil works or qualification of the existing barriers and doors to withstand flooding could be considered.

3.2.1.3 ALARP Option 3: Achieve an Operator Action

109 The consideration of operator actions as a form of mitigation for potential flooding events is recognised, however, the need for classified and redundant detection and alarm systems is identified to satisfy the requirements of the safety case. As a result the single

failure criterion is applied for equipment used in the mitigation of flooding events e.g. sensors and valves.

110 There are further requirements associated with operator actions identified within the submission, specifically, accessibility both in terms of potential flood water and radiological restrictions. Should a valve be located within an area where access is prohibited due to radiological conditions, the valve cannot be claimed as part of the mitigation for flooding.

111 Finally, the feasibility of the option is dependent upon whether there is sufficient time for the operator to undertake the action and considers whether the action can be undertaken from the MCR or locally on plant. The submission only considers this aspect qualitatively as a specific substantiation of the human based safety claims has been undertaken within Reference 22.

3.2.2 Analysis of the ALARP Options

112 The submission considers the above ALARP options on a building by building basis and details the mitigation in place against the worst case flooding scenarios identified within Section 3.1 of this report.

3.2.2.1 Reactor Building Containment (HRA)

113 There were two systems identified within the Reactor Building Containment that could result in an initiating flooding event resulting in exceeding the building retention volume, namely:

- An ND50 pipe break in the SED system, and
- An ND100 pipe leak in the CCWS system.

114 For the ND50 pipe break in the SED system, the ALARP analysis identifies that options 1 and 3 could be viable and that Option 2 would not serve to provide mitigation of the flooding initiator given the unlimited upstream volume of water.

115 Option 1 associated with the provision of an engineered solution considered the practicability associated with sleeving the pipework, but was discounted due to the impact on the design coupled with the ability to inspect the pipework contained within the sleeve. The potential for dry pipework was also discounted given that the SED system supplies water to the primary system for make-up of demineralised water to the reactor coolant pump (RCP) systems. The ability to automatically isolate the SED on detection of a flooding event was considered and the following modifications were identified in order for this option to be effective:

- Integration of additional classified sensors in order to rely on an automatic detection that would allow clear identification of the flooding initiator.
- Modification of the instrumentation and control system to close the relevant isolation valve following pump tripping, if required.
- Replacement of manual isolation valves by motorised ones.

116 The submission identifies that this option could be possible as there is no safety impact, but recognises the need for further analysis to identify in greater detail the impact on the design.

117 Option 3 associated with the provision of operator actions considers both the means by which to detect and isolate the flooding event arising from failure of the SED. Currently the SED has no classified means by which to detect flooding and is reliant on the level

detection within the IRWST reaching the MAX1 level, which would not identify the failed system. In relation to isolation, it would be possible to perform a preventive isolation of the SED in order to prevent dilution of borated water within the IRWST. In order to achieve this one of two valves would need to be closed; one valve is motorised and can be closed from the MCR and the other is a manual valve which would require a local operator action within room [redacted] of the Fuel Building. As the valves are located outside of the Reactor Building Containment the flooding event would not compromise access to the valves. In accordance with the application of the single failure criterion, the motorised valve is assumed to fail. If this were to occur there would be approximately 12 hours for the operator to perform the isolation manually prior to the water reaching the [redacted] level within the Containment (the IRWST is considered as being full of borated water initially).

118 For the ND100 pipe leak in the CCWS system, the ALARP analysis identifies that options 3 could be viable and that Option 1 would not be practicable given the significant impact on layout and civil structures. Dry pipework would also not be an option due to the safety classified function of the CCWS. The analysis does identify that the automatic isolation of the CCWS is already in place, however, this only actuates if the leak rate is greater than [redacted]. Option 2 would not serve to provide mitigation of the flooding initiator given the unlimited upstream volume of water.

119 Option 3 considers the method by which a leak would be detected and identified by the operators. In addition to the level detection within the NVDS sump, the lowering of the level of the CCWS tank and provided the SED volume is displayed in the MCR, the operator would be alerted of a potential CCWS leak. In order to isolate the leak there would be a need for the four F2 classified motorised valves to be closed to mitigate the flooding scenario. With the application of the single failure criterion (one CCWS valve is assumed to fail) the SED in the affected SAB could be isolated locally in order to remove the supply to the CCWS. All the manual valves that could be required to be isolated locally are located outside of the Reactor Building Containment. In order to meet the requirements of the single failure criterion, the submission identifies that the manually operated SED valves should be reclassified to be F2. Given that there is 175 hours before the level within the Containment reaches the [redacted] level, the submission states that it would be possible for an operator to perform the mitigation actions.

120 The ALARP analysis concludes that given the analysis of the options available, Option 3 associated with operator actions is considered to be the ALARP solution for all bounding cases in the Reactor Building Containment.

3.2.2.2 Reactor Building Annulus (HRB)

121 Further to the analysis undertaken within Reference 14, the submission considers the potential impact on safety classified SSCs within the Reactor Building Annulus (HRB). The submission identifies that there is redundant F2 classified level detection within the NVDS sumps which would trigger an alarm within the MCR should the sump high level (MAX2) be reached. This alarm, like the other NVDS sump alarms, would not identify the flooding initiating system.

122 Within the Reactor Building Annulus there is no requirement for water-tightness between the divisions as there is no segregation between the divisions within the area. It is stated that there are safety classified systems contained within HRB and at levels significantly lower than the maximum flood heights postulated. As a result, there is a need for a specific analysis to be undertaken for HRB.

123 The F1 safety classified equipment contained within HRB is associated with Heating Ventilation and Air Conditioning (HVAC) systems, specifically the Annulus Ventilation System (AVS) and the Controlled Safeguard Building Ventilation System (CSBVS). The lowest section of HVAC is the [redacted] steel duct which is located at [redacted] above the concrete basement floor at [redacted]. The AVS air heaters are located at higher level. The maximum acceptable flood height within HRB is at approximately [redacted], which equates to a maximum permissible flood volume of [redacted].

124 Further to the information relating to the safety classified equipment identified in the previous paragraph, studies have been performed to determine what systems would exceed the maximum water level. In a number of cases systems have been discounted due to either double sleeving of the penetration pipework or have water volumes less than [redacted]. The following systems have been identified that could result in a flood volumes that could exceed the maximum acceptable water level and hence impact the CSBVS within HRB:

- Nuclear Island Fire Protection System (JPI).
- Demineralised Water System (SED).
- Fuel Pool Cooling System (FPCS).
- Reactor Coolant System (RCS)

125 The four systems identified above have been analysed within the submission and the following scenarios have been identified where failure could result in the worst case flood for each system:

- ND50 pipe break in the JPI system.
- ND50 pipe break in the SED system.
- ND150 pipe leak in the FPCS.
- ND50 pipe break in the RCS seal return line.

126 The outcome of the ALARP optioneering for each of the scenarios in HRB is shown below:

Scenario	ALARP Option					
	1	Engineering Solution	2	Enhance Barriers	3	Operator Action
ND50 Break in JPI	✘	**Double Piping** – not reasonable given the length of pipework and maintenance disadvantages. **Dry Pipework** – not possible given need for fire fighting system within HRB. **Automatic isolation** - not viable as there may be a real demand on the system in the event of fire.	✘	Not applicable as it would not mitigate the flooding event due to unlimited upstream volume.	✓	There would be less than one hour to isolate assuming a worst case flow rate of [redacted]. **Detection**: a combination of automatic start of the JAC pumps from redundant F2 classified pressure sensors and through the sump detection within HRB. **Isolation**: achieved through redundant manual valves on the JPI system classified F2. In some cases there are motorised valve classified

Scenario	ALARP Option					
	1	Engineering Solution	2	Enhance Barriers	3	Operator Action
						either F1B or F2. In all situations the operator would need to confirm that there was no fire prior to isolating the JPI.
Conclusion	*"Six valves at least need to be closed locally in order to isolate the JPI supply in the Annulus. Assuming the failure of one of the first isolation valves, ten valves at most need to be closed (applying the single failure). As most of the manual action valves require a local action and are located in different areas, the feasibility of these manual actions within the given time (one hour) seems difficult and needs to be substantiated by a human factor analysis.* *Modifications (such as replacement of manual valves by motorised ones) would have to be considered if the human factors analysis results are not acceptable. In the NSL phase, other design options such as dry pipework and automatic isolation might also be considered if the JPI system requirements are modified in order to take into account UK specific requirements (such as classification differences and fire fighting requirements)."*					
ND50 Break in SED	✘	**Double Piping** - not reasonable given the impact on the civil design, length of pipework, and maintenance disadvantages. **Dry Pipework** – not possible as the SED supplies demineralised water to the primary system. **Automatic isolation** – could be considered as it has no immediate impact on safety. In order for this option to be effective the following modifications would be required: ■ Additional classified sensors in order to rely on automatic detection for clear identification of the flooding initiator. ■ Modification of the C&I to close the relevant isolation valve following pump tripping, if required. ■ Replacement of manual isolation valves by motorised ones.	✘	Not applicable as it would not mitigate the flooding event due to unlimited upstream volume.	✓	There would be less than one hour to isolate assuming a worst case flow rate of [redacted]. **Detection**: the SED system has no dedicated classified detection and the water will flow into the NVDS sump in HRB. There would be an alarm within the MCR, but this would not reveal the system that had failed. **Isolation**: a preventive manual isolation is recommended following flood detection in the annulus as it will have no impact on nuclear safety. Two SED lines would need to be isolated in the HRB, however, access would not be compromised by the flooding event as they are located outside the RB. Three valves at most would need to be closed, taking into account the single failure criterion.
Conclusion	*"The feasibility of these actions within the given time (one hour and ten minutes) must be assessed in a specific human factor analysis. Modifications (such as replacement of manual valves by motorised ones) or other options would have to be reconsidered if the human factors analysis results are not acceptable."*					
ND150 Leak in FPCS	✘	**Double Piping –** might be possible as there are only two FPCS penetrations in the HRB.	✘	Not applicable as it would not mitigate the flooding event due to unlimited upstream volume.	✓	There would be approximately 3.5 hours to isolate assuming a worst case flow rate of

Scenario	ALARP Option					
	1	Engineering Solution	2	Enhance Barriers	3	Operator Action
		Impacts on the layout and civil work and needs to be assessed during the Site Specific Phase. **Dry Pipework** – not applicable as these pipes are used during normal plant operations during specific stages such as filling and draining of the RB pool. **Automatic isolation** – already designed with automatic interlocks that can only be activated during fuel loading and unloading phases. If the level of the pool decreases to the MIN1 level then the FPCS valves would close automatically, however, this would not occur during IRWST purification or filling and drainage of the reactor pool before and after refuelling.				[redacted]. **Detection**: in addition to the level detection for the NVDS sumps in the Reactor Building annulus, the operator would be alerted to a break in the FPCS by the discrepant water levels in the reactor pool and the IRWST, which are both displayed in the MCR' **Isolation**: during reactor pool drainage there would be a need for one operator action to close all the FPCS valves from the MCR. In the case of reactor pool filling or IRWST purification, only the FPCS discharge line is used. There is an F1 classified motorised valve located within the FB that can be used to mitigate the flooding event following FPCS pump trip. On applying the single failure criterion to this valve, there are further F2 classified motorised valves located within the SAB that can be closed to isolate the supply from the IRWST. These operator actions can be undertaken from the MCR.
Conclusion	*"These operator actions seem reasonably achievable within the given time (3.5 hours)"*					
ND50 Break in RCS Seal Return Line	✘	**Double Piping –** might be possible as this option is already used for other RCV lines in the Annulus. This option impacts the civil design and layout and needs to be assessed in detail during the Site Specific Phase. **Dry Pipework** – not possible as this function is used during normal plant operation. **Automatic isolation** – already integrated in the RCV system but dependent upon the overflow generated, however the automatic interlocks would not be triggered in the case of small leaks below the sump high level (MAX2).	✘	Not applicable as it would not mitigate the flooding event due to unlimited upstream volume.	✓	There would be approximately 40 hours to isolate assuming a worst case flow rate of [redacted]. **Detection**: would be performed by the NVDS sump level sensors and F2 classified sensors in the RCV lines in the FB. **Isolation**: there are redundant F1B classified motorised valves located within the Reactor Building Containment which can be closed from MCR.

Scenario	ALARP Option					
	1	Engineering Solution	2	Enhance Barriers	3	Operator Action
Conclusion	*"These operator actions seem reasonable achievable within the given time (approximately 40 hours)."*					

127 The ALARP analysis concludes that, for the Reactor Building Annulus, that Option 3 is the most appropriate ALARP option for each of the four cases. However the first two options require human factors analysis given the short period of time for the actions to be performed. Should the results of the human factors analysis not be acceptable the submission identifies that design modifications such as replacement of manual valves by motorised ones or increasing the allowable flood height in the annulus would have to be considered. This is identified as a task to be considered in the Site Specific Phase in order to take into account UK site conditions and specific requirements in systems design.

3.2.2.3 Fuel Building (FB)

128 For each of the breaks and the leaks, the optioneering undertaken followed the same detailed approach to the analysis undertaken for the Reactor Building Containment and Annulus. From the analysis undertaken within Reference 14, three flooding scenarios were identified within the Fuel Building that required detailed ALARP analysis:

- ND50 pipe break in the JPI system.
- ND50 pipe break in the SED system.
- ND100 pipe leak in the CCWS.

129 The timescales for action are significantly longer than for the worst case flooding scenarios within the Reactor Building Annulus with the minimum time for operator action being 12 hours in the case of an ND50 pipe break in the JPI system.

130 The review of the ALARP options cites safety classified sensors and valves as well as the means by which operators would be made aware of the source of the flooding initiator for example the automatic start of the JAC pumps together with the notification by the level sensors within the NVDS sumps.

131 Given the extended timescales for operator action, the analysis concludes that Option 3 is the most appropriate ALARP option.

3.2.2.4 Safeguard Auxiliary Buildings (SAB)

132 For each of the breaks and the leaks, the optioneering undertaken followed the same approach to the detailed analysis undertaken for other buildings analysed. From the analysis undertaken within Reference 14, eight flooding scenarios were identified within the Safeguard Auxiliary Buildings that required detailed ALARP analysis:

- ND50 pipe break in the SEP system.
- ND50 pipe break in the JPI system.
- ND700 pipe leak in the ESWS.
- ND50 pipe break in the SED system.
- ND25 pipe break in the SER system.
- ND300 pipe leak in the CHRS.
- ND100 pipe leak in the CCWS.

- ND80 pipe leak in the CCWS.

133 The timescales for action are significantly longer than for the worst case flooding scenarios within the Reactor Building Annulus with the minimum time for operator action being 17 hours in the case of an ND50 pipe break in the SEP system within SAB2 or SAB3.

134 As was the case for the other buildings, the review of the ALARP options cites safety classified sensors and valves as well as the means by which operators would be made aware of the source of the flooding initiator for example notification by the level sensors within the NVDS sumps together with the need for a preventative isolation of the SEP system following flood detection via the NVDS sumps.

135 Given the extended timescales for operator action, the analysis concludes that Option 3 is the most appropriate ALARP option.

3.2.2.5 Diesel Buildings (DB)

136 For each of the breaks and the leaks, the optioneering undertaken followed the same approach to the detailed analysis undertaken for other buildings analysed. From the analysis undertaken within Reference 14, three flooding scenarios within the Diesel Buildings were identified that required detailed ALARP analysis:

- ND50 pipe break in the JPV system.
- ND25 pipe break in the SED system.
- ND25 pipe break in the SEP system.

137 The most significant flooding scenario is associated with an ND50 pipe break in the JPV which results in a minimum time for operator action of approximately 4 to 5 hours in the SBO diesel buildings. The timescales associated with the pipe breaks in the SED and SEP systems are considerable longer with a minimum time for operator action of 20 hours.

138 Within each of the diesel buildings, there are [redacted] sumps with classified level sensors which would enable operators to identify flooding within a specific diesel building, however, they would not be able to identify the specific system that had failed.

139 The ALARP analysis for the SED and SEP systems is included within the submission, however, I have not repeated the detail within this report given the extended timescales associated with operator action. The ALARP analysis for the JPV system is detailed below given the relatively short period of time required for operator action.

140 Option 1 associated with designing an engineering solution in order to mitigate the worst case flooding event associated with an ND50 pipe break in the JPV system considers double piping, utilising dry pipework, and automatic isolation. The option of double piping of the JPV system would eliminate the flood risk but is discounted given the large length of pipework, the difficulties associated with maintenance and inspection, and the significant impact on layout and civil work. The option of utilising dry pipework is already applied to the JPV pipework downstream of the following deluge valves:

- [redacted] and [redacted] in Diesel Building A (HDA).
- [redacted] and [redacted] in Diesel Building B (HDB).
- [redacted] and [redacted] in Diesel Building A (HDA) Station Black-Out Diesel compartment (SBO).

141 Consequently, only a leak or break in the JPV part upstream of these valves could generate a flooding event. French national requirements do not permit the fire fighting system to be dry during operation given the fire fighting requirement of the system. The submission recognises that such requirements may be different for the UK EPR™ design and may be studied in greater detail during the Site Specific Phase.

142 Automatic isolation of the JPV is not considered appropriate for the JPV fire fighting system as it required in the event of a fire within the building.

143 Option 2 associated with the provision of enhanced divisional barriers is discounted given that increasing the height of the barriers would not eliminate the risk as the upstream volume of the JPV is considered to be unlimited.

144 Option 3 associated with operator actions identifies that the time to operator action considers that they are penalising as no account is taken of head losses in the pipework in the JPV system. The means by which the flooding event would be detected within the diesel buildings is associated with the automatic start of the classified fire fighting water supply system (JAC) pumps. Each JAC train is equipped with F2 classified pressure sensors which would inform operators in the MCR of starting of the JAC pumps, however, it would not identify the location of the failure in the JPV. The means by which the location of the failure would be known to the operators is through the classified level sensors located within the sumps in each of the diesel buildings alarming within the MCR. With both these pieces of information available to operators within the MCR, they would be able to identify the source of the flooding event. The analysis states that manual valves would need to be closed in order to isolate the flooding event. The valves required to be closed in the event of a failure in the JPV can be operated from outside the affected diesel building. Prior to operation of the valves the operator is required to confirm that no fire has started in the relevant diesel building.

145 The ALARP analysis concludes that Option 3 is the most appropriate ALARP option. It identifies that two valves must be closed in order to isolate the JPV supply in one diesel division. With the single failure criterion applied with one of the isolation valves, there would be a requirement to close up to three more valves. As a result a maximum of six valves would need to be closed to isolate the JPV in one diesel division. As the manual valves are located within different areas coupled with the time available for isolation (4-5 hours), the submission recognises the need for substantiation through a human factors analysis. It identifies that should the outcome of the human factors analysis not be acceptable there would be a need to consider modifications such as replacement of manual valves with motorised ones.

3.2.2.6 Nuclear Auxiliary Building (NAB)

146 For each of the breaks and the leaks, the optioneering undertaken followed the same approach to the detailed analysis undertaken for other buildings analysed. From the analysis undertaken within Reference 14, five flooding scenarios were identified within the Nuclear Auxiliary Building that required detailed ALARP analysis:

- ND50 pipe break in the SEP system.
- ND50 pipe break in the JPI system.
- ND50 pipe break in the SED system.
- ND100 pipe leak in the CCWS.
- ND150 pipe leak in the SER system.

147 The timescales for action are significantly longer than for the worst case flooding scenarios within the Reactor Building Annulus with the minimum time for operator action being 30 hours in the case of an ND50 pipe break in the SEP system.

148 As was the case for the other buildings, the review of the ALARP options cites safety classified sensors and valves as well as the means by which operators would be made aware of the source of the flooding initiator for example notification by the level sensors within the NVDS sumps together with the need for a preventative isolation of the SEP system following flood detection via the NVDS sumps.

149 The submission concludes that Option 1 associated with automatic isolation could be considered for the SED, SEP, and SER systems as it would have no adverse impact on safety. The impact of the potential modifications on the reference design could be significant in comparison to the benefit gained given the time available for mitigation through operator actions. The options associated with double piping and dry pipework identify that the risk of flooding could be eliminated, however, these options are not considered reasonably practicable. As a result of the extended timescales for operator action, the analysis concludes that Option 3 is the most appropriate ALARP option.

3.3 UK EPR™ - Internal Flooding – Multi-legged safety case and ALARP consequence assessment analysis, ECEIG121115 Revision B

150 The above submission (Ref. 16) was provided by EDF and AREVA further to the assessment of the first two submissions. The ONR assessment by internal hazards, fault studies, structural integrity, and human factors identified that the approach taken was inconsistent with ONR expectations due to the assumption of leak rather than break for classified moderate energy pipework with a nominal diameter greater than 50mm. This further deliverable presented multi-legged arguments and an ALARP consequence analysis associated with internal flooding. The submission considers the consequences of gross failure of classified moderate energy pipework with a nominal diameter greater than 50mm (ND>50mm). The consequence analysis includes:

- Methodology applied to perform the consequence assessments.
- Scope of the work to be undertaken within the analysis.
- The selection of representative cases in which pipe failure and subsequent flooding is postulated.
- In the event of unacceptable consequences, identification of potential design modifications.
- ALARP assessment of the design options to determine a preferred design solution.

151 The consequence analysis identifies that the current design is robust against the effects of flooding arising from gross failure of moderate energy systems with the exception of the following two systems:

- Fire fighting system (JPI) pipework in the Annulus (HRB).
- Essential Service Water System (ESWS) pipework in the Safeguard Auxiliary Buildings (SAB).

152 In addition, the demineralised water system (SED) has been subject to further analysis given that failure of a 50mm pipe section within HRB constitutes a major flood initiator which could result in flood water affecting redundant safety significant systems in just over one hour.

153 For each of the above systems, design modifications have been identified as a result of the further analysis undertaken.

154 Within the submission there are arguments presented within each of the following areas:

- Design Quality Level for Procurement.
- Maintenance: Quality Manufacture and 60 Year Life of Plant.
- Operational Feedback.
- Mitigation Measures.

3.3.1 Design Quality Level for Procurement

155 The quality measures for procurement states that the pipework quality is based upon the mechanical classification of the system utilised on the FA3 project. The classification and categorisation for UK EPR™ is expected to change during the Site Specific Phase as a result of the application of the findings of the GDA Issue, GI-UKEPR-CC-01. However, the submission states that the pipework will be procured to a high quality commensurate with relevant specifications derived from internationally accepted standards and best practice. In addition, there are to be specific programmes of inspection and quality assurance applied during the procurement of the pipework to be installed within the facility.

156 The section concludes that the design conception and procurement give assurance that limits the occurrence of gross failure in moderate energy classified pipework and that the basis of the design of classified moderate energy pipework can be assumed to be a crack which results in a leak. However, the submission recognises that consequences of gross failure of pipework need to be considered within the multi-legged safety case.

3.3.2 Maintenance: Quality Manufacture and 60 Year Life of Plant

157 The maintenance requirements of the pipework throughout the 60 year life of the plant are to be established during the Site Specific Phase and will include periodic external inspection as well as further inspections such as non-destructive testing depending upon the situation and sensitivity of the system involved.

3.3.3 Operational Feedback

158 EDF operational experience has shown that, apart from failures due to major and direct impacts, only leaks occurred in moderate energy pipework. However, many of the existing fire protection systems (JPI) installed across the EDF fleet are constructed of carbon steel and are prone to corrosion. The existing JPI systems across the EDF fleet use only raw water, whereas, the EPR™ design uses demineralised water with chemical conditioning to ensure that the pH is above 9. In addition, there have been no occurrences of gross failure of JPI systems across the fleet despite occurrences of general corrosion.

3.3.4 Mitigation Measures

159 The submission cites a number of mitigation measures in place in the event of flooding. These measures are split into three areas:

- Detection: each classified building has redundant classified sump level measurements with their associated alarms displayed in the Main Control Room (MCR). For some specific systems there are additional alarms displayed within the MCR.

- Isolation: each fluid system has isolation valves (manual or motorised from the MCR). The classification and redundancy of the alarms are detailed further within the analysis provided within the submission, an overview of which is provided later within this report.
- Human factors: Task analyses to demonstrate the feasibility and reliability of performing representative isolation tasks are performed in order to validate the operator mitigation actions.

160 In all cases where there are redundant isolation valves they are geographically separated from each other and in many cases located within different buildings to minimise the potential for common cause failure due to a single flooding event.

161 In addition to the mitigation measures identified above, the design also considers the need for the systems to be appropriately classified and categorised to withstand seismic events.

162 For the areas detailed above (3.3.1 to 3.3.4) the submission concludes that the claims and arguments presented provide assurance that the design will limit the risk due to internal flooding in safety classified buildings even in the case of gross failure of pipework. In order to complete the safety case a detailed consequence assessment has been undertaken as gross failure of pipework cannot be discounted, however, it recognises that such events would be extremely infrequent.

3.3.5 Consequences Assessment

163 The March 2011 Consolidated PCSR (Ref. 10) postulated double ended guillotine break (DEGB) for the following systems:

- High energy pipework.
- Moderate energy classified pipework with a ND≤50mm.
- Moderate energy non-classified pipework.

164 As consequence analyses on pipework where DEGB is postulated have already been undertaken, the submission focuses on DEGB for moderate energy classified pipework with an ND>50mm within safety classified buildings, namely, the Reactor Building, Fuel Building, Safety Auxiliary Buildings, and the Diesel Buildings.

165 The consequence assessments have been performed to avoid any potential cliff-edge effects and have the following safety objectives:

- The consequences of flooding do not induce a core melt.
- For the Fuel Building, fuel assemblies must stay under water.
- For radiological consequences, analyses are limited to the prevention of a release to the environment.
- Prevent jeopardising the divisional segregation. The loss of a second division could be justified but this would be on a case by case basis.

166 The following assumptions are applied within the consequence analyses undertaken:

- Gross failure is considered for components and systems with no restrictions on the break size.
- A realistic flow rate is assumed, which is based on system operational conditions such as pressure, head loss, pump capacity etc.

- Non-classified systems are not considered for mitigation actions (detection and/or isolation) except when adequately justified.
- No analysis of potential flow paths inside buildings is performed and as a result, the released volume is assumed to flow to the lowest level of the building.
- Watertight doors are assumed to fail in advance of the barrier in which they are contained.

3.3.5.1 Analysis of the Reactor Building, Fuel Building, and Diesel Buildings

167 Each building has been subject to a consequence analysis which has considered the worst case flooding scenarios.

168 The Reactor Building is essentially two buildings, the Containment and Annulus. The Annulus has been subject to a separate more detailed analysis given the potential flooding sources, as detailed within Section 3.3.5.2. No scenarios have been analysed for the Containment for the following reasons:

- Provision of automatic isolation and any released volume is bounded by PCC3/4 transient scenarios which have already been studied,
- And/or, the released volume as a result of failure is contained within the In-Containment Refuelling Water Storage Tank (IRWST).
- The systems are normally dry, are not used, or have a limited volume,
- The nominal diameter of the pipework is less than 50mm and hence has already been evaluated.

169 For the Fuel Building and Diesel Buildings the following table identifies the systems that are postulated to fail. The time to unacceptable consequences and the number of valves required to be closed are included within the following table.

Building	System	Nominal Diameter (mm)	Retention Volume m^3	Flowrate (m^3/h)	Time	No. of Valves	
						Motorised	Manual
Fuel Building	**JPI**	200	[redacted]	[redacted]	5h 40min	0	4
Fuel Building	**SED**	100	[redacted]	[redacted]	5h 40min	0	2
Diesel Building	**JPV**	150	[redacted]	[redacted]	2h 38min	SBO (1) HDA (1) HDB (0)	SBO (1) HDA (2) HDB (2)

170 The submission states that the timescales would be considerably longer due to the limited make-up rates and conservatism in flow rates applied, however, the human factors task analyses that has been undertaken (Ref. 22) demonstrate that the requisite actions can be performed with a margin of greater than 2 hours for the most onerous flooding scenarios for the Fuel Building. The Diesel Building has a limited margin given the need to close more valves, however, given the conservatism that has been applied together with the geographical separation of the two Diesel Buildings, the submission concludes that this is acceptable.

3.3.5.2 Analysis of the Reactor Building Annulus

171 The analysis identifies that the Annulus has not been specifically sized for internal flooding events and recognises that there are exceptions to divisional segregation. Furthermore, it recognises that there are safety redundancies located at a level significantly lower than the maximum flood height within the Annulus. As a result a specific analysis is required for this area to ensure that common mode failure cannot occur as a result of an internal flooding event.

172 The safety classified redundancies that are located beneath the maximum flood height are the Annulus Ventilation System (AVS) heaters and the Controlled Safeguard Building Ventilation System (CSBVS) ventilation duct. The ventilation duct, [redacted], is at the lowest level and hence most vulnerable, and is located [redacted] from the concrete floor at level [redacted].

173 The retention volume within the Annulus has been calculated as the volume between the concrete floor and the lowest level redundant equipment (the CSBVS duct). Allowance is taken for the duct itself, the concrete walls and floors, and [redacted] for the volume of equipment. This results in a retention volume within the Annulus of [redacted]. This is greater than the previous calculation of [redacted] as detailed within Reference 15 due to the more detailed calculation undertaken as part of the analysis within Reference 16.

174 The following table identifies the scenarios that are postulated to result in the most significant flood volumes. The flow rate, the potential released volume, and the time to unacceptable consequences are included within the table.

Scenario	System and Operating State	Flowrate (m^3/h)	Potential Released Volume m^3	Time
HRB1	ND150mm DEGB in JPI.	[redacted]	[redacted]	39 min
HRB2c	ND150mm DEGB in FPCS suction line (reactor pools drainage).	[redacted]	[redacted]	41 min
HRB3c	ND150mm DEGB in FPCS discharge line during reactor pool drainage.	[redacted]	[redacted]	1h 46min
HRB3d and e	ND150mm DEGB in FPCS discharge line during filling of the reactor pool, or IRWST purification.	[redacted]	[redacted]	3h 33min
HRB3f	ND150mm DEGB in FPCS discharge line penetration in HRB.	[redacted]	[redacted]	8h 27min

175 For HRB1, the HRB sump alarm, [redacted], would be activated quickly and would notify operators within the MCR. Also, in a very short period of time, the two fire fighting water supply (JAC) pumps would also start-up due to the pressure drop in the JPI. With both pieces of information, operators would be made aware the source of the flooding scenario. In order to isolate the system six valves would need to be closed locally within 39 minutes. The analysis recognises that this timescale would be insufficient to perform the necessary mitigation actions and identifies that design modifications are required. Appendix 2 of Reference 16 provides the ALARP analysis for the selection of design modifications for the JPI system within the Annulus, namely:

- Option 1: Do nothing.

- Option 2: Limit the flow rate of the fire fighting system through the introduction of a bypass line at the entrance of the Nuclear Island. This option would result in a lower flow should there be a failure of the pipe within the Annulus as the main line would be isolated unless confirmation of fire is provided to MCR.
- Option 3: Decrease the time to perform mitigation actions through changing a number of valves from manual to motorised as well as provide new motorised valves controlled remotely from the MCR.
- Option 4: Decrease the time to perform mitigation actions through the automatic isolation of the fire fighting system within the Reactor Building Annulus following leak detection from the fire fighting system.
- Option 5: Enhance the hazard barriers by raising the height of vulnerable redundancies, namely the CSBVS duct. Valve closure of the JPI system would be performed locally by the operator after leak detection within HRB.
- Option 6: Use double walled piping for the JPI system within HRB or by designing and manufacturing the pipework such that it could be treated as a High Integrity Component (HIC).
- Option 7: Mitigation through separating the hose reels from the sprinkler systems within HRB:
  - For the hose reels, a preventive automatic isolation will be included which would actuate in the event of detection of flooding within the NVDS sump and the automatic start of the JAC pumps due to a drop in pressure in the line.
  - For the sprinkler system, an automatic isolation signal which would actuate 20 minutes after the detection within the NVDS sump and the automatic start of the JAC pumps.
- Option 8: Modification of the JPI system such that the system is dry operated on pressure drop in the event of actuation of a sprinkler head. Hose reels would be opened and filled by fire fighters locally when necessary.

176 Each option was scored in terms of safety and commercial benefits and dis-benefits. Examples of the types of safety benefits included within the ALARP scoring:

- Deterministic safety requirements fully met,
- Reduction in radiological risk,
- Improves resistance to hazards,
- Improves segregation and separation.

177 The analysis scored Option 7 the highest and concluded that this together with Option 3 should be taken forward into the design for UK EPR™. These options are included as part of the modification detailed within the Change Management Form (CMF), CMF56 (Ref. 20).

178 As was the case for HRB1, should the scenario, HRB2c, occur the sump alarm would be activated quickly and notify operators within the MCR. IRWST level information displayed within the MCR would alert the operator of a leak/break within FPCS during these specific phases. In addition, due to a drop in suction pressure, the pumps used to drive the water will be automatically tripped with a further alarm raised within the MCR. In order to terminate the flood, three motorised valves need to be close from the MCR and with the application of the single failure criteria, a further valve would be required to be closed.

The submission recognises that for the event to occur there would be a need for the concurrent failure of the line at the time when the system when is in use specifically for drainage of the reactor building pools. This is a short duration operational task that normally occurs twice during each refuelling outage, which take place typically every 12, 18, or 22 months. During this time, there is monitoring of reactor pool drainage by operators. The analysis recognises the limited length of pipework affected in this scenario, together with the limited time period when the discharge line is operated together with assuming failure of the line, coupled with the MCR operation of the motorised valves via pressing a single button. The submission concludes that the provisions in place to isolate the flooding are ALARP.

179 For the remaining scenarios, HRB3c, 3d, 3e, and 3f, the analysis concludes that the flood would be detected and identified through MCR notification of sump level alarms together with IRWST level indication and that the timescales and associated valve operation would be achievable without further modification.

180 In addition to the scenarios identified above, failure of a ND50 pipe in the demineralised water system (SED) within the Annulus had been identified previously (Ref. 14) and the need for further mitigation was identified. Within Appendix 1 of the submission, an ALARP case for the design modifications was undertaken. The consequence analysis (Ref. 15) identified that there was 1 hour and 9 minutes before water levels would threaten redundant safety classified systems. The analysis deemed this timescale was insufficient to perform the necessary mitigation actions and identifies that design modifications are required.

181 Appendix 1 provides the ALARP analysis for the selection of design modifications for the SED system within the Annulus, namely:

- Option 1: Do nothing.
- Option 2: Double walled piping for the SED as it is routed through HRB to supply HRA.
- Option 3: Automatic isolation of the SED following detection of flooding within HRB. One valve would need to be changed from manual to motorised, and a new C&I signal would need to be created to implement this option.
- Option 4: Change a number of valves from manual to motorised, controlled from the MCR in order to decrease the time to close isolation valves. Valve closure of the SED system would be performed by an operator from within the MCR on leak detection within HRB and on diagnosis of the SED pipework failure.
- Option 5: A modification of the operator procedure to include a preventive isolation of the SED on flooding detection within HRB. Valve closure of the SED system would be performed locally by the operator.
- Option 6: Enhance the hazard barriers by raising the height of vulnerable redundancies, namely the CSBVS duct. Valve closure of the SED system would be performed locally by the operator after leak detection within HRB.

182 As with the JPI ALARP analysis, each option was scored in terms of safety and commercial benefits and dis-benefits. The analysis scored Option 5 the highest and concluded that this together with Option 4 should be taken forward into the design for UK EPR™. These options are included as part of the modification detailed within CMF58 (Ref. 20).

3.3.5.3 Analysis of the Safeguard Auxiliary Buildings

183 As mentioned previously, there are four Safeguard Auxiliary Buildings (SABs) within the Nuclear Island which are vertically divided with the levels beneath [redacted] level used for water retention in the event of flooding. No exceptions to divisional segregation exist between each of the SAB, therefore, the analysis focuses on potential flooding scenarios that result in exceeding the retention volumes at the [redacted] level.

184 For each scenario the time to perform mitigation actions is calculated. If the flooding level is neither detected, nor isolated, the entire volume of the tanks upstream the break considered in the system is assumed to be released. For systems fed by seawater no limitation exists on the volume released.

185 The following table identifies the DEGB scenarios within each of the SABs that are postulated to result in the most significant flood volumes. The flow rate, potential released volume, and the time to unacceptable consequences are detailed within the following table:

Scenario	System	Nominal Diameter (mm)	Flowrate (m^3/h)	Potential Released Volume m^3	Allowed time to perform mitigation actions in SAB			
					1	2	3	4
HL1	JPI	200	[redacted]	[redacted]	≈16h	≈13h	≈13h	≈15h
HL2	ESWS	700	[redacted]	[redacted]	38min	36min	36min	37min
HL3	SED	80	[redacted]	[redacted]	≈30h	≈28h	≈28h	≈30h
HL4	SER	150	[redacted]	[redacted]	-	-	-	≈10h
HL5	UCWS	300	[redacted]	[redacted]	5h 09min	-	-	-

186 Scenarios HL1, HL3, HL4, and HL5, have been shown to result in a considerable time period before divisional segregation is compromised and as a result the submission states that operator mitigation action can be achieved within the timescales calculated.

187 The submission states that the time to achieve mitigation through local operator action for scenario HL2 are not considered sufficient and as a result design modifications need to be implemented. Appendix 3 of Reference 16 provides the ALARP analysis for the selection of design modifications for the ESWS system within the SABs, namely:

- Option 1: Do nothing.
- Option 2: Modify the C&I of the ESWS to have an automatic isolation of the ESWS upstream of the SAB entrance. The signal related to this automatic isolation would be based on detection via the high level alarm (MAX2) in the NVDS sump in the considered SAB.

- Option 3: Add or modify existing valves to have a motorised isolation valve on each ESWS line, in order to perform mitigation actions from the MCR following detection via the NVDS sump alarm.
- Option 4: On flooding detection via the NVDS sump alarm, the corresponding ESWS pump is tripped from the MCR.
- Option 5: The addition of a dedicated alarm to detect high flow rate internal flooding. This could be implemented via a new high level NVDS sump alarm, locally higher than the MAX2 existing NVDS high level sump alarm. Mitigation actions are performed locally or from the MCR (trip the associated ESWS pump).
- Option 6: Enhance the hazard barriers by making the divisional barriers above [redacted] level watertight. Mitigation actions are performed locally by the operator after leak detection in the SAB and diagnosis of ESWS pipework failure.

188 As with the JPI ALARP analysis, each option was scored in terms of safety and commercial benefits and dis-benefits. The analysis scored Option 5 (mitigation action from the MCR) the highest and concluded that this together with Option 4 should be taken forward into the design for UK EPR™. These options are included as part of the modification detailed within CMF57 (Ref. 20).

189 The ALARP analysis recognises the short timescales associated with mitigation actions for the ESWS and states:

"It will be necessary for future licensees to carry out more detailed assessments of grace periods, time to perform mitigation actions and consequences of delayed mitigation when there is improved information available, in order to determine a more realistic margin and also to confirm that the operator action can be performed with adequate reliability when considered with the assessed consequence. If these additional studies do not provide an acceptable result then it will be necessary to implement a design change for automatic trip of the ESWS pump on detection of flooding in the associated SAB."

190 The report identifies that no further reasonably practicable measures have been identified to further limit the consequences of an ESWS failure in a SAB, however, further work will be performed during the Site Specific Phase to substantiate that this Human Based Safety Claim is sufficiently reliable.

3.3.6 Conclusions of the Multi-legged safety case and ALARP consequence assessment analysis, ECEIG121115 Revision B

191 The multi-legged safety case has required the following input information to ascertain the risks to the UK EPR™ as a result of internal flooding:

- Evaluation of maximum flow rates,
- Identification of bounding cases,
- Demonstration that mitigation actions for each of the cases are achievable and manageable,
- Demonstration that the consequences of the flooding event are acceptable.

192 DEGB of classified moderate energy pipework with a ND>50mm has identified unacceptable consequences for the following two systems:

- Fire fighting system (JPI) pipework in the Annulus.
- Essential Service Water System (ESWS) pipework in the Safeguard Auxiliary Buildings (SABs).

193 Detailed ALARP analyses have been provided for each of the above systems together with proposed design modifications.

194 In addition, unacceptable consequences associated with failure of ND50 pipework associated with the demineralised water system (SED) within the Annulus were identified within References 14 and 15 and the submission details the ALARP analysis of proposed design modifications.

195 The submission concludes:

"In order to provide substantiation to the design, flooding scenarios have been considered with no restrictions on failure mode. It has been demonstrated that, for each case evaluated with regard to DEGB, the safety consequences are acceptable with the initial design proposed or with the implementation of reasonably practicable design modification that has been identified using an ALARP evaluation."

4 ONR ASSESSMENT

196 Further to the assessment work undertaken during Step 4 (Ref. 6), and the resulting GDA Issue GI-UKEPR-IH-03 (Ref. 5), this assessment focuses on the claims, arguments and evidence associated with the need to provide an adequate safety case for internal flooding. The identified EDF and AREVA deliverables are intended to provide the requisite claims, arguments and evidence and are detailed within the Resolution Plan (Ref. 7) provided at the end of Step 4 of GDA.

197 This assessment has been carried out in accordance with the ONR HOW2 document PI/FWD, "Permissioning - Purpose and Scope of Permissioning" (Ref. 1).

4.1 Scope of Assessment Undertaken

198 The scope of the assessment has been to consider the expectations within the GDA Issue, GI-UKEPR-IH-03, and the associated GDA Issue Action which is detailed within Annex 3 of this report. As explained previously substantiation of the internal flooding safety case through a deterministic analysis assuming an unmitigated flood source was required. The response to the GDA Issue Action required EDF and AREVA to produce multi-legged arguments with consideration given to the following aspects:

- Potential failure mechanisms of water based systems.
- Civil engineering aspects including barriers and drainage.
- Systems (both engineered and administrative) to ensure that the effects of an internal flooding event are limited to loss of one division.
- Any further defence in depth and ALARP measures that could be implemented into the design.
- The impact of the changes made to the PCSR relating to the outcome of this substantiation on other safety case submissions such as civil engineering and human factors.

199 The scope of this assessment is not to undertake further assessment of the PCSR nor is it intended to extend this assessment beyond the expectations stated within the GDA Issue Actions, however, should information be identified that has an affect on the claims made for other aspects of internal hazards such that the existing case is undermined, these have been addressed.

4.2 Assessment

200 The three submissions provided to support closure of this GDA Issue summarised within Sections 3.1, 3.2, and 3.3 have been subject to assessment within this section of my report.

4.2.1 Internal Flooding – Identification of bounding cases: leak volumes and retention volumes, ECEIG110718 Revision A

201 The above submission (Ref. 14) details a thorough approach to the identification of the bounding cases with all the potential flooding initiators reviewed in the first instance. Consideration has been given to the potential flow rates and available water stocks. It conservatively assumes that there are no head losses within the pipework, which is a good approach to take to identify the major flood initiators. A further positive aspect of the analysis is the conservative assumption that if there are automatic make-up systems, an unlimited flood volume is assumed. There is consideration of the retention volumes, level monitoring sensors, automatic isolation, and MCR alarms to identify whether the potential

flooding initiator is a major flood source. The report has identified a number of systems and flooding scenarios that are taken forward into the second task associated with mitigation measures and ALARP optioneering.

202 One aspect of the identification of major flooding initiators is the assumption that leaks are postulated for classified moderate energy pipework with a ND>50mm. This claim was challenged as part of this assessment as the arguments presented were not in line with my expectations and the expectations of ONR Structural Integrity specialists for unmitigated flood sources.

203 As part of the assessment of the claims made for non-classified Q3 quality piping, TQ-EPR-1467 (Ref. 13) entitled, *"QA Standards for Failures of Non-Classified Moderate Energy Pipework"* was raised as part of the assessment. The TQ requested:

- *"Please supply the failure assumptions coupled with the assessment of the quality assurance requirements applied to the JPI system pipework to demonstrate that failure of pipework DN>50mm can be discounted from the analysis."*

204 The response to the TQ stated:

"The failure assumptions for pipework are detailed in Sub-Chapter 13.2 of the UK EPR PCSR and are consistent with IAEA Safety Standard NS-G-1.11 [1]. They depend on:

- the pressure / temperature of the relevant system, which results in the high or moderate energy classification,

- the pipe diameter,

- and the pipework quality level, design and manufacturing rules.

Sub-Chapter 13.2 of the PCSR states within Section 3.2.2:

"Leaks are generally postulated for classified moderate energy pipework (DN > 50).

Breaks are postulated for small diameter pipework (DN < 50).

For non-classified moderate energy pipework, in accordance with Sub-chapter 3.2, there is generally no limit with regard to the size (up to break) and the location of the failures. However, based on the assessment of the material, fluid, in-service inspections, etc, failure assumption restrictions may be applied on a case by case basis, if necessary."

In the internal flooding report related to the GDA issue IH03 (Ref. ECEIG110718), all input data used to perform this analysis are coming from the Flamanville 3 Project design, including buildings size and systems data such as classification.

In the Flamanville 3 EPR, the JPI system is F2 safety classified but mechanically non-classified (M1/M2/M3) as it does not have a barrier function for radiological containment. Its failure cannot result in a radioactivity release significantly greater than that existing in the surrounding environment. However the JPI pipework is supplied and manufactured in the same design quality level as a M3 classified pipework.

Moreover, the JPI fire fighting network system is the subject to controls and periodic tests (Sub-Chapter 9.5 of the PCSR, section 1.3.5.4). In addition to these tests, maintenance and in service inspection of the JPI system should be performed to ensure the durability of the quality level for the lifetime of the plant.

Based upon the requirements related to the design, manufacturing, in-service monitoring and inspection, the JPI system pipework is equivalent to M3 classified pipework, except that its contents are not radioactive.

Regarding the threshold value for break assumption, it originates from a German and French regulators workshop. In view of the EPR conceptual safety features which recommended to increase from DN 25 (regular French practice) to DN 50 (German practice) the size of piping for which break should be postulated at all locations.

A double ended guillotine break of larger DN moderate energy pipework is not considered credible due to the lower pressure / temperature (lower stresses within the pipe and insufficient energy to generate pipe motion), material characteristics, design standards, manufacturing quality controls as well as the construction, operation, maintenance and inspection regimes."

205 Whilst the IAEA guidance, NS-G-1.11 (Ref. 4) does recognise that claims can be made associated with leak rather than break in pipework with a ND>50mm and bases the leak size on the pipe thickness multiplied by the diameter divided by four (Dt/4), it doesn't address the expectations of the HSE SAPs and those of ONR Structural Integrity Assessors.

206 Discussions took place with EDF and AREVA to ascertain the basis of the claims for these specific systems in order to obtain the requisite evidence to support the break preclusion claims in this instance. ONR Structural Integrity and Fault Study Assessors were involved in the discussions associated with the assessment in this area.

207 A letter (Ref. 17) was sent to EDF and AREVA reiterating the ONR's expectations:

- *"Unless a component is identified as a High Integrity Component (HIC), then there needs to be a consequences case.*
- *The consequences case needs to consider gross failure.*
- *It may be appropriate to use realistic assumptions in assessing the consequence case, but that does not extend to classing a small leak as a gross failure"*

208 The letter requested that EDF and AREVA provide details of the approach to be adopted for the failures of moderate energy pipework with a diameter greater than 50mm including both classified and non-classified pipework.

209 EDF and AREVA's response (Ref. 18) proposed the production of a multi-legged safety case and ALARP analysis that considered breaks in all moderate energy pipework with an ND>50mm and would include development of the following claims:

- Origin and conservative assumptions for the ND50 criteria.
- Consistency criterion for international safety standards.
- Design quality level for procurement and manufacturing to ensure gross failure limitation.
- In-service monitoring requirements, controls, periodic tests and maintenance (over 60 years) that could be required for operation.
- Measures put in place to ensure that the impact of the flooding generated by gross failure is minimised.
- A consequence assessment considering gross failure of pipework to provide confidence that the provisions in place to ensure that the risk to nuclear safety of the consequences of gross failure are ALARP.

210 The response proposed studying the Reactor Building Annulus (HRB) and one Safeguard Auxiliary Building (SAB) in the first instance and cites the following reasons for their selection:

"The Annulus has been chosen as a representative building due to exceptions to divisional segregation and concerns with regard to achievability of the mitigation action claims applied to the flooding case (see letter EPR70404R). One of the Safeguard Buildings has been selected because of its high nuclear safety importance and because preliminary assessment indicates that the available/current mitigation is relatively limited."

211 The response states that for completeness, the other buildings of the Nuclear Island will be analysed during the Site Specific Phase.

212 Any options for design changes that could be implemented to prevent loss of more than one division are to be identified and an ALARP assessment undertaken to identify those that will be implemented into the design. Those taken forward will be captured within Stage 1 Change Modification Forms (CMFs) in order for them to be integrated in the end of GDA design reference.

213 The analysis for HRB and one of the SABs was provided within the submission, "*UK EPR™ - Internal Flooding – Multi-legged safety case and ALARP consequence assessment analysis, ECEIG121115"* (Ref. 16), the details of which, are summarised within Section 3.3 and assessed within Section 4.2.3 of this assessment report.

214 I was satisfied with the EDF and AREVA response to my letter that stated ONR's expectations with regard to the consideration and approach to addressing gross failure of moderate energy pipework with a ND>50mm.

215 Overall, the submission provided a detailed review of potential flooding initiators and identified the major flooding sources within each of the Nuclear Island buildings, however, given that the basis of the flood volumes in relation to leaks in moderate energy pipework with an ND>50mm has been challenged by ONR, the need to consider more onerous flooding scenarios was identified.

4.2.2 Internal Flooding – Bounding cases: mitigation measures, ECEIG111647 Revision B

216 As was the case with the previous submission, *"Internal Flooding – Identification of bounding cases: leak volumes and retention volumes, ECEIG110718"* (Ref. 14), the above submission (Ref. 15) utilised the claim associated with leak as opposed to break for pipework with an ND>50mm when calculating flow rates and flood volumes. I, therefore, chose to assess the ALARP process applied to the optioneering to determine the adequacy of the approach and identify whether there were any aspects of the current ALARP analysis that did not meet ONR expectations. The need to consider the consequences associated with pipe break is addressed within the submission "*UK EPR™ - Internal Flooding – Multi-legged safety case and ALARP consequence assessment analysis, ECEIG121115"* (Ref. 16).

217 It was important to note that the scenarios associated with requirement for operator action within the Reactor Building Annulus for both the JPI and SED systems would be challenging. I would have expected further passive or active engineered protection systems to have been implemented within this area and did not accept the approach of utilising a human factors analysis to ascertain "acceptability" in the first instance. I believed that it would be ALARP during the design stage to engineer protection such that challenging operator actions were not included within the design. I consulted with colleagues within Human Factors and Fault Studies Assessment areas and they concurred with my opinion in that the approach to the ALARP analysis in this area was too dependent upon operator action without due consideration of other, more reliable,

methods such as passive and active protection. This concern was communicated to EDF and AREVA within the same letter as mentioned above (Ref. 17) which stated:

"I have reviewed the revised bounding flooding analysis document that you submitted on the 26th January, which now includes the Reactor Building Annulus. I have discussed the submission with colleagues in fault studies, human factors, and ONR Management and we have concluded that the provisions in place are not ALARP. This is primarily associated with claims made relating to operator actions. Whilst we recognise that some alternative options are presented, we are not satisfied that they have been subject to sufficiently detailed analysis prior to being discounted. Furthermore, these aspects are clearly associated with the generic UKEPR design and as such it is not acceptable for them to be considered solely within the site specific design."

218 EDF and AREVA agreed to consider the ALARP options, as detailed within Section 3.3 of this report, as part of the further submission providing a multi-legged safety case for internal flooding as the flow rates and volumes were to be subject to change as a result of the consideration of breaks in pipework with an ND>50mm.

219 Notwithstanding the above, the detailed ALARP analysis, which followed on from the identification of the flooding scenarios, considered each of the potential flooding initiators in detail. As part of the analysis, the three options available for each of the scenarios included detailed consideration of the system and operational requirements. The approach was comprehensive and the impact of each of the options analysed has considered the safety impact of both implementation of the option as well as the wider safety implications of changing the design. I am satisfied that the approach to the ALARP analysis was well structured and the selection of the most suitable option had a clear basis.

4.2.3 UK EPR™ - Internal Flooding – Multi-legged safety case and ALARP consequence assessment analysis, ECEIG121115 Revision B

220 The above submission (Ref. 16) provides further detailed analysis addressing DEGB of classified moderate energy pipework with a ND>50mm together with associated ALARP analyses for the two identified systems which could result in unacceptable consequences. In addition the ALARP analysis considered failure of the demineralised water system (SED) within the Annulus, which had previously been identified as resulting in unacceptable consequences should there be a DEGB of the pipework.

221 The approach taken to the consequence analysis for gross failure of classified moderate energy pipework with a ND>50mm has adopted a systematic approach to the identification of potential flooding initiators followed by consideration of the retention volumes in which the water would be released. This allowed for the timescales for mitigation action, if any, to be determined. The next step considered exceptions to segregation such as the Annulus and Fuel Building in order to ascertain whether the potential for common mode failure existed. Finally, a detailed analysis was performed to determine whether the mitigation actions were achievable within the timescales available. If the outcome highlighted insufficient time for mitigation actions, design modifications were proposed. I am satisfied that this approach served to identify any potential threats to the redundancy fundamental to preventing common cause failure of plant and equipment due to internal flooding.

222 Using the above approach, the safety classified buildings within the nuclear island were subject to analysis. The analysis that was performed provided substantiation for each of the buildings.

223 I am satisfied that no further analysis requires to be undertaken associated with gross failure of classified moderate energy pipework with a ND>50mm within the Reactor Building Containment given the bounding nature of the PCC3/4 events for the systems identified. In addition, there are limited additional water sources coupled with the provision of alarms within the MCR, such as level monitoring of the IRWST, which would notify operators of a flooding event given that the flood water would ultimately drain into the IRWST.

224 I am satisfied with the approach taken to the identification of the flooding sources within the Fuel Building and Diesel Building given the relatively long time for operator action and the geographical separation of the Diesel Buildings, and have not undertaken any further assessment of flooding within either of these two buildings.

225 The consequences analysis for the Reactor Building Annulus has considered the threat to safety redundancies arising from flooding initiators and used the height of the lowest redundancy as well as applied conservatism in ascertaining the retention volume. By applying the methodology mentioned earlier, the analysis identified the most onerous timescales by which mitigation had to be undertaken for a number of the systems within the Annulus. The effectiveness of the methodology has resulted in the identification of the need for design modifications within this area which have been subject to ALARP analysis. The two ALARP modifications for the Annulus are associated with the fire fighting system (JPI) and the demineralised water system (SED). Further to the submission of the ALARP analysis, the following Change Management Forms (CMFs) were submitted to ONR for assessment with a view to inclusion within the Design Reference for UK EPR™:

- CMF 56 (Ref. 20)
- CMF 58 (Ref. 20)

226 CMF 56 relates to changing seven manual valves to motorised ones that can be operated automatically in the event of sump level detection and operation of the classified fire fighting water supply system (JAC) pumps. In addition, a further four motorised valves have been added to take into account single failure. The additional electrical and control and instrumentation (C&I) has also been identified for both the change from manual to motorised valves and for the new motorised valves. Finally, a two step isolation signal for the hose reels and sprinkler system within the Annulus has been introduced to ensure that it is automatically isolated 20 minutes after flood detection by the sump level measurement in order to ensure that flood levels do not result in loss of more than one redundant safety significant system. This automatic isolation after 20 minutes ensures that the automatic fire fighting system (sprinkler system) is operational for a sufficient period to support the fire fighting strategy in case of “internal flooding” spurious signal. The categorisation and classification of the proposed modifications are to be undertaken during the Site Specific Phase. As this modification does not involve any operator actions, given the automatic nature of the isolation of both the hose reels and the sprinkler system within the Annulus, no Human Factors input was required.

227 CMF 58, associated with the Demineralised Water System (SED), consists of changing from a manual valve to one that is motorised. Again, the electrical and C&I aspects are considered, as is the need to consider the categorisation and classification of the proposed modification during Site Specific Phase. There are also changes to the operational procedures associated with the need to perform a preventative isolation in the event of detection of flooding via the level detection identified within CMF56.

228 I have discussed the multi-legged safety case (Ref. 16) and the modification, CMF58, with human factors specialists and they have confirmed (Ref. 21) that they are satisfied as this modification was subject to assessment as part of the task analysis submission (Ref. 22) provided by EDF and AREVA for assessment as part of close out of GI-UKEPR-HF-01. The task analysis produced by EDF and AREVA identified that the existing operator actions involved in the isolation of this system would take approximately 2 hours 25 minutes against a required time of 1 hour and 9 minutes. It judges that the isolations involved are equivalent to high risk due to their importance to the deterministic safety case requirements. As a result the task analysis recommended that the valves be changed from manual to motorised valves operated from the MCR. This is, therefore, in line with the modifications proposed by EDF and AREVA within the multi-legged safety case (Ref. 16) and the subsequent CMF, CMF58 (Ref. 20)

229 I am satisfied that the approach to the identification of flooding initiators, the subsequent consequence analysis, and the proposed design modifications have been adequately analysed and that the proposed modifications for the annulus are ALARP.

230 Flooding as a result of a failure of the ESWS within a SAB building was identified as a system which could result in unacceptable consequences within a short period of time (≈36 minutes). The approach taken to the consequence assessment was the same as that previously and proved to be effective in identifying the unmitigated consequences of failure of the ESWS. The consequence assessment highlighted the need for design changes given that the operator mitigation actions were not considered sufficient.

231 Option 2, associated with a modification to the control and instrumentation (C&I) of the ESWS to include automatic isolation of the ESWS train upstream of the SAB entrance may still be progressed as further human factors consideration is deemed to be required during the Site Specific Phase. Should this option be progressed, the submission states that the valves would have to be F1 safety classified and that when the UK classification was applied during the Site Specific Phase it is likely to result in the level sensors being classified as Class 1. Option 2 impacts on material, classification and has a major impact on the complexity of the C&I. The optioneering identified this modification as difficult to implement, however, the submission stated that if the human based safety claims could not be substantiated it would require further consideration during the Site Specific Phase.

232 As this option may require further consideration during the Site Specific Phase and given that it would have an impact on the classification of the C&I, I sought advice from Fault Studies specialists and they confirmed that should this option be taken forward there would be a need to use the PSA model developed in response to **AF-UKEPR-PSA-035** to consider the balance of risk for these two options prior to making a definitive decision on which option to implement.

233 Ultimately options associated with provision of additional level detection and improved operator procedures including preventive isolation of the ESWS on detection of flooding were taken forward as the ALARP options for this scenario.

234 Further to the submission of the ALARP analysis, the following CMF was submitted to ONR for assessment with a view to inclusion within the Design Reference for UK EPR™:

- CMF 57 (Ref. 20)

235 CMF 57 relates to additional flood level detection and preventative pump trip of the Essential Service Water System (ESWS) within the Safeguard Auxiliary Buildings. Sensors are to be placed [redacted] above the floor at the [redacted] level in each of the SABs to ensure that should failure of the ESWS occur then there is sufficient time and

relevant information for operators to realign the ESWS onto a different division and to isolate the affected ESWS in advance of water reaching the [redacted] level.

236 Again, I have discussed the multi-legged safety case (Ref. 16) and the above modification with Human Factors specialists within ONR and they recognise the need for the substantiation to be developed once more information is available during the Site Specific Phase. Their assessment states (Ref. 21):

"The assessment and conclusions appear appropriate – it suggests that the leak isolation actions are likely to be feasible on relatively short timescales providing that leak isolation actions are readily identifiable from the indications generated and procedural guidance provided. There needs to be consideration of automation of these actions as indicated in the HFIR [Human Factors Issues Register] to determine the most appropriate ALARP option. If reliance on manual actions is the preferred option then this will require detailed justification and verification of the HMI [Human Machine Interface] and procedural issues post-GDA"

237 In addition, they have raised an Assessment Finding **(AF-UKEPR-HF-58)** relating to the potential for internal flooding such as failure of the ESWS to generate alarms which are likely to mask or delay the response. Furthermore, the modification was subject to assessment by Fault Studies specialists within ONR and they considered the proposed modification within their assessment (Ref. 19).

238 I am content with the proposed modification recognising the potential impacts on the functionality of the ESWS and the impact on the C&I of automatic isolation of a safety system. The further analysis work that is to be undertaken by a future licensee should enable the balance of risk of failure of the ESWS against the impact of automating the system to be informed by the PSA for internal flooding mentioned earlier. Given that this potential flooding initiator has yet to be fully resolved, I have elected to raise an assessment finding to ensure that it is captured during the Site Specific Phase:

> ***AF-UKEPR-IH-14:*** *The Licensee shall ensure that the detailed analysis of the Human Based Safety Claim associated with isolation of the ESWS is undertaken. In the event that it cannot be substantiated the option relating to automatic isolation of the ESWS should adequately consider the balance of risk associated with automatic isolation of a safety system as well as the associated classification of that system.*
>
> ***Required timescale:*** *"Mechanical, Electrical, and C&I Safety Systems – Before inactive commissioning"*

239 Given the impact on the fault schedule and potential for flooding to affect multiple safety classified systems, I requested assessment of the submission (Ref. 16) by ONR Fault Studies specialists who provided me with an assessment (Ref. 19) which concluded:

"The report identifies the bounding flooding scenarios due to double-ended guillotine breaks (DEGB) of moderate energy pipework for the UK EPR and provides a consequence assessment for these cases together with an assessment of potential modifications to demonstrate that the risk is ALARP. The report is well argued and systematic and I am generally content with its conclusions. I consider that sufficient information has been provided to justify closure of GDA Issue ***GI-UKEPR-IH-03*** *from a fault studies perspective."*

240 The arguments presented associated with the quality of the design and manufacture of the pipework are comprehensive. However, the classification and categorisation of the pipework as well as the systems in place for detection and isolation of potential flooding

scenarios will require review in accordance with UK categorisation and classification expectations and will need to be addressed during the Site Specific Phase.

241 The fault studies assessment (Ref. 19) identified one recommendation for an Assessment Finding to be raised associated with categorisation and classification of the automatic isolation. The assessment report (Ref. 19) stated:

"The report screens out a number of flooding scenarios on the basis that the system associated with the piping failure will be automatically isolated following detection of leak. Some of the detection and isolation systems claimed are not Class 1 systems. An Assessment Finding should be raised requiring a future licensee to review these scenarios and to either provide additional consequence cases for these scenarios or upgrade the classification of these detection and isolation systems to Class 1 during the categorisation and classification work to be performed during NSL."

242 I have reviewed the recommendation and concur that it should be captured as Assessment Finding:

> ***AF-UKEPR-IH-15:*** *The Licensee shall review the potential flooding scenarios that require automatic isolation following detection of a leak or break and provide substantiation of the classification and categorisation of those systems.*
>
> ***Required timescale:*** *"Mechanical, Electrical, and C&I Safety Systems – Before inactive commissioning".*

243 In addition, there is a need to ensure that my expectations in relation to claims made for leak of the pipework rather than break are captured within the site specific safety case during the Site Specific Phase. I have, therefore, raised an assessment finding to ensure the explicit need for the internal flooding safety case to capture gross failure of classified moderate energy pipework with a ND>50mm and not just leak arguments based upon Dt/4.

> ***AF-UKEPR-IH-16:*** *The Licensee shall ensure that the site specific safety case for internal hazards captures the need to consider gross failure of classified moderate energy pipework with a nominal diameter greater than 50mm rather than claiming leak equivalent to the diameter multiplied by the thickness divided by 4 (Dt/4).*
>
> ***Required timescale:*** *"Mechanical, Electrical, and C&I Safety Systems – Before inactive commissioning"*

244 I am content with the design changes proposed for UK EPR™ and believe that such changes will result in a more robust safety case in the event of gross failure of systems contained within the SAB and Annulus.

245 Overall, I am satisfied that the submission provided detailing the multi-legged safety case and ALARP consequence assessment is a detailed and thorough analysis of the internal flooding initiators arising from failure of classified moderate energy pipework with a ND>50mm. The approach taken to the arguments presented within the multi-legged case is in line with my expectations in relation to the SAPs and relevant good practice. This information presented within the multi-legged safety case together with that contained within References 14 and 15 provide a robust safety case for internal flooding for the UK EPR™.

4.3 Comparison with Standards, Guidance and Relevant Good Practice

246 The following SAPs have been used to inform my assessment and an analysis is provided against each in relation to the UK EPR™ design:

Engineering principles: key principles	Safety measures	EKP.5
Safety measures should be identified to deliver the required safety function(s).		

"Safety should be secured by characteristics as near as possible to the top of the list below:

a) Passive safety measures that do not rely on control systems, active safety systems or human intervention.

b) Automatically initiated active engineered safety measures.

c) Active engineered safety measures that need to be manually brought into service in response to the fault.

d) Administrative safety measures (see paragraph 376 f.).

e) Mitigation safety measures (e.g. filtration or scrubbing).

Note: The hierarchy above should not be interpreted to mean that the provision of an item towards the top of the list precludes provision of other items where they can contribute to defence in depth."

247 The submissions (Refs. 14 - 16) provided in response to this GDA Issue has confirmed that the design hierarchy within EKP.5 has been addressed in the design of UK EPR™ given that the overriding principle is associated with the passive physical segregation of redundant safety classified plant and equipment. Where this has not been achieved detailed analyses have been provided that follow the principles of EKP.5 which demonstrate that there would be no loss of redundant safety classified equipment as a result of an internal hazard. There is one Assessment Finding associated with EKP.5 which require a future licensee to ensure that the human based safety case claims associated with ESWS failure are completed and if not judged acceptable implement further more robust means by which to isolate, namely through automatic isolation **(AF-UKEPR-IH-14).**

Engineering principles: safety classification and standards	Standards	ECS.3
Structures, systems and components that are important to safety should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to the appropriate standards.		

"The standards should reflect the functional reliability requirements of structures, systems and components and be commensurate with their safety classification."

248 There is confidence that the pipework within the UK EPR™ design will be to a high standard, however, the UK categorisation and classification process is to be undertaken during the Site Specific Phase. Given the deterministic nature of the analysis of the unmitigated consequences of pipework failure, the safety case for internal flooding has been shown to be robust.

Engineering principles: external and internal hazards	Fire, explosion, missiles, toxic gases etc – sources of harm	EHA.14
Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed.		

249 This SAP has been fully addressed through the production of an unmitigated consequences safety case for internal flooding.

Engineering principles: external and internal hazards	Fire, explosion, missiles, toxic gases etc – effect of water	EHA.15
The design of the facility should prevent water from adversely affecting structures, systems and components important to safety.		

"The design of the facility should include adequate provision for the collection and discharge of water reaching the site from any design basis external event or internal flooding hazard or, if this is not achievable, the structures, systems and components important to safety should be adequately protected against the effects of water."

250 The design of the UK EPR™ has demonstrated the provision of retention volumes and has considered such volumes within the unmitigated consequences analysis that has been undertaken.

Engineering principles: reliability claims	Engineered safety features	ERL.3
Where reliable and rapid protective action is required, automatically initiated engineered safety features should be provided.		

"For requirements that are less demanding or on a longer timescale, operator actions or administrative control may be acceptable to complement the engineered systems. The objective should be to minimise the dependence on human action to maintain a safe state."

251 This SAP has been adequately addressed through the analysis work undertaken associated with detection, isolation (both manual and automatic), and the consideration of operator actions including detailed analysis of the extent of work required. There is an Assessment Finding associated with this SAP associated with the need for a future licensee to review the potential flooding scenarios that require automatic isolation following detection of a leak or break and provide substantiation of the classification and categorisation of those systems **(AF-UKEPR-IH-15)**.

Engineering principles: design for reliability	Redundancy, diversity and segregation	EDR.2
Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components important to safety.		

252 The UK EPR™ design for internal flooding adequately addresses the expectations of this SAP through the provision of divisional segregation and the provision of water tight barriers between redundant items of safety classified plant and equipment. The only areas where there is no segregation provided is within the Reactor Building Containment and Reactor Building Annulus. There are adequate arguments in place associated with bounding scenarios within the Reactor Building Containment such that failures of pipework within the area would not lead to consequences which are not already considered already within the safety case. The submissions presented associated with the Reactor Building Annulus have provided arguments and proposed modifications to ensure that no more than one redundant safety classified system is lost as a result of an internal flooding event.

Engineering principles: design for reliability	Single failure criterion	EDR.4
During any normally permissible state of plant availability no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function.		

253 The application of a single random failure has been applied within the internal flooding safety case and demonstrates that the design is robust to both a single random failure and a concurrent internal hazard.

254 With regard to discounting gross failure of pipework, there is information contained within the section of the SAPs associated with Structural Integrity. Paragraph 243 of the SAPs detail ONRs expectations in relation to the production of a safety case through discounting gross failure:

"Discounting gross failure of a component or structure is an onerous route to constructing a safety case. Such a case should provide in-depth explanation of the measures over and above normal practice that support and justify the claim. If discounting gross failure cannot be justified, it may be possible to consider a case based on consequences (see paragraph 246)."

255 Paragraph 246 of the SAPs state:

"Where:

a) the case cannot meet the level needed for a claim that the likelihood of a failure event can be discounted, and

b) all practical avenues to improve the structural integrity case have been exhausted;

the basis of the safety case needs to be revisited and the consequences of gross failure of components or structures explicitly considered. This would potentially involve a site-specific evaluation of short and long-term off-site consequences and would still require some estimate of the reliability of the components or structures in question. This broadening of the basis of the safety case would clearly require involvement of disciplines in addition to structural integrity."

256 The internal flooding safety case for UK EPR™ now takes into account gross failure of moderate energy pipework with a ND>50mm and has shown through a comprehensive consequences analysis that, with the incorporation of three modifications, that the case can withstand such failures.

257 The UK EPR™ design has shown that the above principles have been addressed from an internal hazards perspective and that the design is robust to the effects of internal flooding as the principles of divisional segregation and redundancy have been demonstrated within the design.

258 NS-G-1.11 (Ref. 5) states within paragraph 3.41 and 3.42:

"It is accepted to postulate only a limited leak (and not a break) if it can be demonstrated that the piping system considered is operated under 'high energy' parameters for a short period of time (e.g. less than 2% of the total operating time) or if its nominal stress is reasonably low (e.g. a pressure of less than 50 MPa).

The locations where a failure has to be postulated should be determined as follows:

(a) At the terminal ends (fixed points, connections to a large pipe or to a component) and at intermediate points of high stress for a piping system designed and operated according to the rules applied for systems important to safety;

(b) In all locations for other pipes.

For piping systems of nominal diameter less than 50 mm, breaks should be postulated at all locations."

259 Furthermore, paragraph 3.47 of Reference 5 states:

"In particular, as well as a break, a leak with a limited area should be considered to be a PIE [Potential Initiating Event] that could lead to an internal flooding hazard[12]. For flange connections and for different types of sealing, the possible leak areas should be analysed case by case."

260 Note 12 within the above extract cites Dt/4 as the basis for the leak size to be assumed.

261 Whilst ONR accept the IAEA guidance and recognise the comprehensive nature and requirements associated with internal flooding, the guidance does not meet our expectations as detailed within the SAPs, specifically, the internal hazards SAP EHA.14 detailed above.

262 The analyses provided in response to this GDA issue has demonstrated that the expectations of the IAEA guidance and the SAPs are met as they have considered the unmitigated worst case flooding initiators including leak times and volumes, drainage routes, design changes, and operator actions.

5 REVIEW OF THE UPDATE TO THE PCSR

5.1 13.2. Internal Hazards

263 Sections 2 and 8 of Chapter 13.2 of the PCSR (Ref. 23) consider protection against pipework leaks and breaks, and internal flooding. The submission was reviewed to ensure that the outcome of the GDA assessment had been appropriately captured therein.

264 There have been changes to the PCSR arising from the assessment that has been undertaken associated with internal flooding, specifically in relation to structural integrity claims for pipework detailed within Section 2.

265 Within Section 8, there is additional reference provided to Section 2 on leaks and breaks and to additional design verification analyses that have been undertaken in the event of an unmitigated internal flooding event. The PCSR also makes reference to the multi-legged safety case and ALARP consequence assessment analysis (Ref. 16) as well as the work undertaken associated with the Human Factors Task Analysis (Ref. 22)

266 I am satisfied that the updated PCSR reflects the findings from the GDA and the text has been updated to reflect the GDA assessment undertaken for close out of this GDA Issue.

6 ASSESSMENT FINDINGS

6.1 Additional Assessment Findings

267 The following Assessment Findings have been raised that requires to be resolved during the Site Specific Phase:

> ***AF-UKEPR-IH-14:*** *The Licensee shall ensure that the detailed analysis of the Human Based Safety Claim associated with isolation of the ESWS is undertaken. In the event that it cannot be substantiated the option relating to automatic isolation of the ESWS should adequately consider the balance of risk associated with automatic isolation of a safety system as well as the associated classification of that system.*
>
> ***Required timescale:*** *"Mechanical, Electrical, and C&I Safety Systems – Before inactive commissioning"*
>
> ***AF-UKEPR-IH-15:*** *The Licensee shall review the potential flooding scenarios that require automatic isolation following detection of a leak or break and provide substantiation of the classification and categorisation of those systems.*
>
> ***Required timescale:*** *"Mechanical, Electrical, and C&I Safety Systems – Before inactive commissioning".*
>
> ***AF-UKEPR-IH-16:*** *The Licensee shall ensure that the site specific safety case for internal hazards captures the need to consider gross failure of classified moderate energy pipework with a nominal diameter greater than 50mm rather than claiming leak equivalent to the diameter multiplied by the thickness divided by 4 (Dt/4).*
>
> ***Required timescale:*** *"Mechanical, Electrical, and C&I Safety Systems – Before inactive commissioning"*

6.2 Impacted Step 4 Assessment Findings

268 No Assessment Findings raised during Step 4 have been impacted as a result of this assessment.

7 ASSESSMENT CONCLUSIONS

269 To recap, the GDA Issue Action stated:

"Please provide adequate substantiation of the internal flooding safety case through a deterministic analysis that initally assumes an unmitigated flood source and applies a multi-legged argument that may include consideration of the following:

- *Potential failure mechanisms of water based systems.*
- *Civil engineering aspects including barriers and drainage.*
- *Systems (both engineered and administrative) to ensure that the effects of an internal flooding event are limited to loss of one division.*
- *Any further defence in depth and ALARP measures that could be implemented into the design.*
- *The impact of the changes made to the PCSR relating to the outcome of this substantiation on other safety case submissions such as civil engineering and human factors."*

270 The deliverables (Refs. 14 - 16) provided in response to this action consider potential flooding initiators within each of the Nuclear Island buildings and determine whether they could exceed the designed retention volumes. The potential failure mechanisms have been extended to include gross failure of all pipework that is not classified as high integrity. The consideration of unlimited water volumes arising from systems that have automatically initiated make-up systems provides further confidence in the approach taken to the analysis. There are claims made on the divisional segregation barriers beneath the [redacted] level to be water-tight which include any associated penetrations, however such penetrations are minimised within the water-tight barriers to minimise the safety challenge to those barriers.

271 There are claims made upon sumps to detect and alarm within the MCR, however, the UK categorisation and classification of those systems are to be determined during the Site Specific Phase. In a number of cases mitigation through operator actions is claimed, however, these have been subject to analysis by human factors specialists within ONR and they are content with such claims. In the event of timescales being too short to claim operator intervention, design modifications have been identified associated with one or more of the following:

- Automatic isolation,
- Replacement of manual valves with motorised ones,
- Enhancement detection and alarm,
- Preventive isolation on detection and alarm of a flooding initiator.

272 The approach to the flooding case has shown from a deterministic basis that should there be a flooding initiator within the Nuclear Island that with the incorporation of modifications in some areas, there is sufficient time for mitigation action to be taken.

273 In conclusion, the totality of the deliverables submitted provide a comprehensive analysis of potential sources of internal flooding within the UK EPR™ and I am satisfied that the safety case for internal flooding is robust. The submissions address the range of potential failure mechanisms, consider the barriers and doors in place to prevent flood propagation affecting more than one redundancy, and include both engineered and administrative measures to mitigate potential flooding events. The analysis has identified reasonably

practicable modifications which result in improvements in the robustness of the internal flooding safety case. I have reviewed the PCSR and am content that it reflects the additional analysis work that has been undertaken in support of the UK EPR™ and am, therefore, satisfied, that the GDA Issue, GI-UKEPR-IH-03, can now be closed.

8 REFERENCES

1 *ONR HOW2. Permissioning - Purpose and Scope of Permissioning.* PI/FWD, Issue 3. HSE. August 2011.

2 *Safety Assessment Principles for Nuclear Facilities.* 2006 Edition Revision 1. HSE. January 2008. www.hse.gov.uk/nuclear/SAP/SAP2006.pdf.

3 *Deterministic Safety Analysis and the Use of Engineering Principles in Safety Assessment.* T/AST/006 Issue 03, HSE, July 2000.

Early Initiation of Safety Systems. T/AST/010 Issue 02, HSE, July 2008.

Internal Hazards. T/AST/014 Issue 02. HSE, August 2008.

Structural Integrity Civil Engineering Aspects. T/AST/017 Issue 02. HSE. March 2005

Diversity, Redundancy, Segregation and Layout of Mechanical Plant. T/AST/036 Issue 02, HSE, June 2009.

Guidance on the Purpose, Scope and Content of Nuclear Safety Cases. T/AST/051 Issue 01, HSE, May 2002

www.hse.gov.uk/nuclear/operational/tech_asst_guides/index.htm.

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

Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants. International Atomic Energy Agency (IAEA), Safety Guide, NS-G-1.11, IAEA, Vienna 2004.

www.iaea.org.

5 *GDA Issue GI-UKEPR-IH-03 Revision 2.* ONR. July 2011. TRIM Ref. 2011/385310. (in TRIM folder 5.1.3.6348.)

6 *Step 4 Internal Hazards Assessment of the EDF and AREVA UK EPR™ Reactor*. ONR Assessment Report ONR-GDA-AR-11-001 Revision 0. TRIM Ref. 2010/581514. (in TRIM folder 4.4.1.1827.).

7 *Resolution Plan for GDA Issue GI-UKEPR-IH-03 Revision 2.* EDF and AREVA. June 2011. TRIM Ref. 2011/256673. (in TRIM folder 5.1.3.6351.)

8 *Reference Design Configuration*. UKEPR-I-002 Revision 13. UK EPR. September 2012. TRIM Ref. 2012/350053.

9 *Design Change Procedure.* UKEPR-I-003 Revision 9. EDF and AREVA. June 2012. TRIM Ref. 2012/243501.

10 *UK EPR GDA Step 4 Consolidated Pre-construction Safety Report – March 2011.* EDF and AREVA. Detailed in EDF and AREVA letter UN REG EPR00997N. 18 November 2011. TRIM Ref. 2011/552663.

11 *Internal Hazards Assessment Plan for GDA Close out of the EDF and AREVA UKEPR™.* ONR, 26 September 2011. TRIM Ref. 2011/560168

12 *EDF and AREVA UK EPR™ - Schedule of Technical Queries Raised during GDA Step 1 to Step 4.* HSE-ND. TRIM Ref. 2010/600726.

13 *EDF and AREVA UK EPR™ - Schedule of Technical Queries Raised during GDA Close-out.* Office for Nuclear Regulation. TRIM Ref. 2011/389411.

14 *Internal flooding – Identification of bounding cases : leak volumes and retention volumes.* ECEIG110718 Revision A, EDF, May 2011. TRIM Ref. 2011/306496

15 *Internal flooding – Bounding cases : mitigation measures.* ECEIG111647 Revision B, EDF, January 2012. TRIM Ref. 2012/48184.

16 *UK EPR™ - Internal flooding – Multi-legged safety case and ALARP consequence assessment analyses.* ECEIG121115 Revision B, EDF, September 2012. TRIM Ref. 2012/377087.

17 *Internal Hazards Associated with Pipework Failure and Flooding.* Letter to EDF and AREVA, EPR70404R, ONR, 15 February 2012. TRIM Ref. 2012/76924

18 *GDA Issue GI-UKEPR-IH-03: EPR70404R - Internal Hazards Associated with Pipework Failure and Flooding.* Response to EPR70404R from EDF and AREVA, EPR01163R, EDF and AREVA, 19 June 2012. TRIM Ref. 2012/244302

19 *GI-UKEPR-IH-03: Assessment of UK-EPR - Internal Flooding – Multi-legged safety case and ALARP consequence assessment analysis – ECEIG121115*. Fault Studies Assessment Note, ONR, 06 November 2012. TRIM Ref. 2012/428676.

20 *Deliverable to GI-UKEPR-CC02 – Action 1- submission programme rev 17.* Letter from EDF and AREVA, EPR01411R, 12 October 2012. TRIM Ref. 2012/401313

CMF56: Internal flooding – Design modification of fire fighting system JPI in the Annulus. Stage 1 CMF, EDF and AREVA, 10 October 2012. TRIM Ref. 2012/401461
CMF57: Internal flooding – Design modification of essential service water system SEC in the Safety Auxiliary Building. Stage 1 CMF, EDF and AREVA, 10 October 2012. TRIM Ref. 2012/401462
CMF58: Internal flooding – Design modification of distribution of demineralised reactor water system (SED) in the Annulus. Stage 1 CMF, EDF and AREVA, 10 October 2012. TRIM Ref. 2012/401464

21 *Assessment notes on EDF/Areva of Operator Actions related to Internal Flooding for GI-UKEPR-HF-01 – document number 16895-707-000-RPT-0013 C-BPE, ONR, June 2012.*. TRIM Ref. 2012/280228

22 *EDF/AREVA GDA Human Factors Internal Flooding.* 16895-707-000-RPT-0013 Revision E, AMEC, September 2012. TRIM Ref. 2012/364866

23 PCSR Sub-Chapter 13.2 Update – Internal Hazards Protection, UKEPR-0002-132 Issue 05, 31st October 2012, TRIM Ref. 2012/450702.

Table 1

Relevant Safety Assessment Principles Considered for Close-out of GI-UKEPR-IH-03 Revision 2

SAP No.	SAP Title	Description
SC.4	Safety case characteristics	A safety case should be accurate, objective and demonstrably complete for its intended purpose.
EKP.3	Defence in depth	A nuclear facility should be so designed and operated that defence in depth against potentially significant faults or failures is achieved by the provision of several levels of protection.
EKP.4	Safety function	The safety function(s) to be delivered within the facility should be identified by a structured analysis.
EKP.5	Safety Measure	Safety measures should be identified to deliver the required safety function(s).
ECS.1	Safety Categorisation	The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be categorised based on their significance with regard to safety.
ECS.2	Safety classification of structures, systems and components	Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance with regard to safety.
EDR.2	Redundancy, diversity and segregation	Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components important to safety.
EDR.4	Single failure criterion	During any normally permissible state of plant availability no single random failure, assumed to occur anywhere within the systems provided to secure a safety function, should prevent the performance of that safety function.

Table 1

Relevant Safety Assessment Principles Considered for Close-out of GI-UKEPR-IH-03 Revision 2

SAP No.	SAP Title	Description
ELO.4	Minimisation of the effects of incidents	The design and layout of the site and its facilities, the plant within a facility and support facilities and services should be such that the effects of incidents are minimised.
EHA.1	Identification	External and internal hazards that could affect the safety of the facility should be identified and treated as events that can give rise to possible initiating faults.
EHA.3	Design basis events	For each internal or external hazard, which cannot be excluded on the basis of either low frequency or insignificant consequence, a design basis event should be derived.
EHA.4	Frequency of exceedance	The design basis event for an internal and external hazard should conservatively have a predicted frequency of exceedance in accordance with the fault analysis requirements (FA.5).
EHA.5	Operating conditions	Hazard design basis faults should be assumed to occur simultaneously with the most adverse normal facility operating condition.
EHA.6	Analysis	Analyses should take into account simultaneous effects, common cause failure, defence in depth and consequential effects.
EHA.7	‘Cliff-edge’ effects	A small change in DBA parameters should not lead to a disproportionate increase in radiological consequences.
EHA.10	Electromagnetic interference	The design of facility should include protective measures against the effects of electromagnetic interference.
EHA.13	Fire, explosion, missiles, toxic gases etc – use and storage of hazardous materials	The on-site use, storage or generation of hazardous materials should be minimised, and controlled and located so that any accident to, or release of, the materials will not jeopardise the establishing of safe conditions on the facility.

Table 1

Relevant Safety Assessment Principles Considered for Close-out of GI-UKEPR-IH-03 Revision 2

SAP No.	SAP Title	Description
EHA.14	Fire, explosion, missiles, toxic gases etc – sources of harm	Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed.
EHA.15	Fire, explosion, missiles, toxic gases etc – effects of water	The design of the facility should prevent water from adversely affecting structures, systems and components important to safety.
EHA.16	Fire, explosion, missiles, toxic gases etc – fire detection and fighting	Fire detection and fire-fighting systems of a capacity and capability commensurate with the credible worst-case scenarios should be provided.
FA.6	Fault sequences	For each initiating fault in the design basis, the relevant design basis fault sequences should be identified.

Annex 1

Deliverables and Associated Technical Queries Raised During Close-out Phase

GI-UKEPR-IH-03 Revision 2 – Internal Flooding Safety Case – EDF and AREVA Deliverables

GDA Issue Action	Internal Hazard	Document Ref.	Title	Ref.
GI-UKEPR-IH-03.A1	Internal Flooding	ECEIG110718 Rev A	Internal Flooding – Identification of bounding cases: leak volumes and retention volumes	14
GI-UKEPR-IH-03.A1	Internal Flooding	ECEIG111647 Rev B	Internal Flooding - Bounding cases: mitigation measures	15
GI-UKEPR-IH-03.A1	Internal Flooding	ECEIG121115 Rev B	UK EPR™ - Internal Flooding – Multi-legged safety case and ALARP consequence assessment analysis.	16

GI-UKEPR-IH-03 Revision 2 – Internal Flooding Safety Case – Technical Queries Raised

TQ Reference	GDA Issue Action	Related Submission	Description
TQ-EPR-1467	GI-UKEPR-IH-03.A1	ECEIG110718	*QA Standards for Failures of Non-Classified Moderate Energy Pipework.*

Annex 2

GDA Assessment Findings Arising from GDA Close-out for Internal Hazards, GI-UKEPR-IH-03

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-IH-14	The Licensee shall ensure that the detailed analysis of the Human Based Safety Claim associated with isolation of the ESWS is undertaken. In the event that it cannot be substantiated the option relating to automatic isolation of the ESWS should adequately consider the balance of risk associated with automatic isolation of a safety system as well as the associated classification of that system.	"Mechanical, Electrical, and C&I Safety Systems – Before inactive commissioning"
AF-UKEPR-IH-15	The Licensee shall review the potential flooding scenarios that require automatic isolation following detection of a leak or break and provide substantiation of the classification and categorisation of those systems.	"Mechanical, Electrical, and C&I Safety Systems – Before inactive commissioning"
AF-UKEPR-IH-16	The Licensee shall ensure that the site specific safety case for internal hazards captures the need to consider gross failure of classified moderate energy pipework with a nominal diameter greater than 50mm rather than claiming leak equivalent to the diameter multiplied by the thickness divided by 4 (Dt/4).	"Mechanical, Electrical, and C&I Safety Systems – Before inactive commissioning"

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

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

Annex 3

GDA Issue, GI-UKEPR-IH-03 – Internal Hazards – UK EPR™

EDF AND AREVA UK EPR™ GENERIC DESIGN ASSESSMENT

GDA ISSUE

INTERNAL FLOODING SAFETY CASE

GI-UKEPR-IH-03 REVISION 2

Technical Area		**INTERNAL HAZARDS**	
Related Technical Areas		Human Factors Civil Engineering Environment Agency	
GDA Issue Reference	**GI-UKEPR-IH-03**	**GDA Issue Action Reference**	**GI-UKEPR-IH-03.A1**
GDA Issue	The internal flooding claims stated within the PCSR appear inconsistent with the deterministic approach to the analysis of potential sources of internal flooding.		
GDA Issue Action	Please provide adequate substantiation of the internal flooding safety case through a deterministic analysis that initally assumes an unmitigated flood source and applies a multi-legged argument that may include consideration of the following: • Potential failure mechanisms of water based systems. • Civil engineering aspects including barriers and drainage. • Systems (both engineered and administrative) to ensure that the effects of an internal flooding event are limited to loss of one division. • Any further defence in depth and ALARP measures that could be implemented into the design. • The impact of the changes made to the PCSR relating to the outcome of this substantiation on other safety case submissions such as civil engineering and human factors. The list above should not be considered to be exhaustive and the items detailed above are provided as a means to inform EDF and AREVA of my expectations. With agreement from the Regulator this action may be completed by alternative means.		