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-FS-04 Revision 0

Steam Generator Tube Rupture Safety Case

Assessment Report: ONR-GDA-AR-12-008
Revision 0
March 2013

COPYRIGHT

EXECUTIVE SUMMARY

This report presents the close-out part of the Office for Nuclear Regulation's (an agency of HSE) Generic Design Assessment (GDA) within the area of Fault Studies (FS) design basis analysis. This report specifically addresses the GDA Issue GI-UKEPR-FS-04 generated as a result of the GDA Step 4, Fault Studies assessment of the UK EPR™. My assessment has focused on the deliverables identified within the EDF and AREVA Resolution Plan published in response to this GDA Issue.

During the GDA Step 4 assessment EDF and AREVA identified that the makeup capacity of the Chemical and Volume Control System (CVCS) is sufficient to compensate for a leakage of up to more than a guillotine break of a single Steam Generator Tube Rupture (SGTR). As such, there would not be an automatic reactor trip on low pressuriser level. This shortfall was the subject of regulatory discussions with EDF and AREVA leading to a proposal to incorporate a design change for the UK EPR™. It was therefore judged that the design basis analyses supporting the revised proposal for the detection and management of the SGTR faults should be revisited within the Pre-construction Safety Report (PCSR). For this reason, GI-UKEPR-FS-04 was raised requiring EDF and AREVA to provide such a case. In particular, the following actions were raised;

- The need to revise the steam generator tube rupture fault safety case to incorporate the proposed design changes identified by EDF and AREVA.
- Provision of human factors analysis to justify the operator actions claimed in the design basis safety case.
- Provision of the transient analysis to demonstrate margin to overfill the affected SG for the design basis Plant Condition Category (PCC), PCC-3 and PCC-4 steam generator tube rupture faults.

In response, EDF and AREVA provided additional information, through a series of analysis reports and responses to technical queries. The main deliverables provided in response to this GDA Issue are a suite of reports which provide the analysis of the steam generator tube rupture fault. This work included the sensitivity study of single tube failure for the UK EPR™, development of a steam generator tube rupture mitigation strategy, a technical note on monitoring the reactor coolant/secondary side leaks for Pressurised Water Reactors, Human Factors (HF) analyses to support operator action claims, and an examination of the international experience feedback supporting the proposed approach.

In order to improve the performance of the SGTR leak detection system for up to and including a guillotine failure of one SG tube, EDF and AREVA have proposed to modify the design and to update the safety case. This modification is captured by a related Change Management Form (CMF #022) with a reliance on detection of increased secondary activity levels to initiate operator action. The proposed design change for the UK EPR™ includes:

- Provision of two redundant Class 1 detection channels on the main steam line on each steam generator. These channels are seismically qualified to meet the requirements of Class 1 safety systems.
- Upgrading to Class 2 safety classification of the activity sampling devices which extracts continuously from the individual blowdown lines for chemical analysis and activity detection. These devices are seismically qualified to meet the relevant classification requirements.

- Reliance on operator actions to initiate a controlled cooldown and reactor trip in response to alarms from the N16 sensors indicating a SG tube leak for leak sizes up to one tube diameter.

In support of the GDA Issue Action 1, EDF and AREVA have provided design basis analysis for the UK EPR™ reference plant to examine the impact of manual reactor trip 50 minutes after the detection of increased radioactivity within the steam line. This approach is supported by operational experience which has been used to formulate the Emergency Operating Procedures (EOP) following SGTR faults to reach the controlled state. The analyses supporting the adequacy of the revised procedures employ UK specific design reference data as expected by the GDA Issue. This analysis is supported by a number of sensitivity assessments to examine the influence of operator action on the development of the transient, and to identify the limiting case regarding the radiological consequences until the leak is gradually terminated.

In addition, EDF and AREVA have identified an additional operator action to prevent steam generator dry out to limit the consequences of radiological release in the SGTR fault conditions.

The human factors supporting analyses and review of operational experience has supported the claims made for manual intervention for SG tube leaks, although several changes to the detailed procedures have been identified to make the operator responses to SGTR faults more robust and reduce the likely time taken to trip manually. These changes have been identified as needing to be incorporated into the appropriate SGTR faults response procedures. The HF submissions covering the changes in the operator actions required by the safety case are assessed to have adequately justified the reliability of the claims being made. This is considered in more detail in the close out report for the Human Factors GDA Issue **GI-UKEPR-HF-01**.

EDF and AREVA have also updated the relevant section of the safety submissions to provide additional analyses demonstrating that there is margin to overfill the affected steam generator for the design basis PCC-3 and PCC-4 SGTR events using the UK specific plant data.

From my assessment, I have concluded that:

EDF and AREVA have performed a satisfactory review of the mitigation strategy aimed at demonstrating a reduction of the radiological risk from the SGTR faults and made significant progress against the detection and management of the steam generator tube rupture faults.

In my opinion, EDF and AREVA have considerably strengthened the design basis safety against the detection and management of the SGTR faults for the UK EPR™ through the additional safety case information and new analysis performed in response to GDA Issue **GI-UKEPR-FS-04**. There are a few areas where additional information needs to be presented or where detailed aspects of the approach require further development. I do not consider these to undermine the validity of the results presented, but I have identified these as areas where additional development in the safety case is required during the detailed design phase as the site specific phase progresses. I have therefore raised the following Assessment Findings to ensure these are resolved satisfactorily by the future licensees to:

- Complete the development work on the optimisation of operator actions claimed to prevent SG dry-out post SGTR faults. The revised proposal is required to fully consider the expectations of Emergency Operating Procedures (EOP) for the UK EPR™.
- Demonstrate that diverse protection is provided for each safety function for frequent SGTR faults.
- Provide a robust justification that the position of the steam line activity sensors is optimised to maximise their sensitivity for detecting the activity released from SGTR faults or to minimise potential radiological discharge to atmosphere.

- Review and update the definition of the “controlled state” for SGTR faults, which is required to ensure that only classified safety protection systems are claimed for minimising the potential discharge to atmosphere.

Overall, based on my assessment undertaken in accordance with ONR procedures, I am satisfied that the safety case for the detection and management of the SGTR faults presented in response to this GDA Issue is adequate subject to satisfactory progression and resolution of the Assessment Findings identified in Annex 1. These are to be addressed during the forward work programme for this reactor. For this reason, I am satisfied that GDA issue **GI-UKEPR-FS-04** can now be closed.

LIST OF ABBREVIATIONS

ALARP	As Low as is Reasonably Practicable
ATWT	Anticipated Transient Without Trip
C&I	Control and Instrumentation
CMF	Change Management Form
CVCS	Chemical and Volume Control System
DAC	Design Acceptance Confirmation
DBA	Design Basis Analysis
EBS	Extra Boration System
EDF and AREVA	Electricité de France SA and AREVA NP SAS
EOP	Emergency Operating Procedures
EFW	Emergency Feed Water
FS	Fault Studies
GDA	Generic Design Assessment
HF	Human Factors
HFAR	Human Factors Assumptions Register
HFIR	Human Factors Issues Register
HMI	Human Machine Interface
HSE	Health and Safety Executive
IAEA	International Atomic Energy Agency
LHSI	Low Head Safety Injection
LOOP	Loss of Offsite Power
MDEP	Multinational Design Evaluation Programme
MFWS	Main Feed Water System
MHSI	Medium Head Safety Injection
MSB	Main Steam Bypass
MSIV	Main Steam Isolation Valve
MSRCV	Main Steam Relief Control Valve
MSRIV	Main Steam Relief Isolation Valve
MSRT	Main Steam Relief Train
NAB	Nuclear Auxiliary Building
NEA	Nuclear Energy Agency
NPP	Nuclear Power Plant
OA	Operator Action

LIST OF ABBREVIATIONS

OECD	Organisation for Economic Co-operation and Development
OL3	Olkiluoto 3
ONR	Office for Nuclear Regulation (an agency of HSE)
PCC	Plant Condition Category
PCSR	Pre-construction Safety Report
PICS	Process Information and Control System
PWR	Pressurised Water Reactor
RCCA	Rod Cluster Control Assemblies
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RHR	Residual Heat Removal
RHRS	Residual Heat Removal System
RP	Requesting Party
RPS	Reactor Protection System
RRC	Risk Reduction Category
RT	Reactor Trip
SAP	Safety Assessment Principle(s) (HSE)
SAS	Safety Automation System
SBLOCA	Small Break Loss of Coolant Accident
SF	Safety Function
SG	Steam Generator
SGa	Affected SG
SGTR	Steam Generator Tube Rupture
SI	Safety Injection
SIS	Safety Injection System
SSC	Systems, Structures and Components
SSS	Start-up and Shutdown System
TAG	Technical Assessment Guide(s) (ONR)
TQ	Technical Query
TSC	Technical Support Contractor
TSN	Taishan
WENRA	Western European Nuclear Regulators' Association

TABLE OF CONTENTS

Tables

Annexes

1 INTRODUCTION

1.1 BACKGROUND

1 This report presents the close-out part of the Office for Nuclear Regulation's (an agency of HSE) Generic Design Assessment (GDA) within the area of Fault Studies (FS) design basis analysis. This report specifically addresses the GDA Issue **GI-UKEPR-FS-04** Revision 1 and associated GDA Issue Actions (Ref. 6) generated as a result of the GDA Step 4 Fault Studies – Design Basis Faults Assessment of this reactor design (Ref. 7). This GDA Issue relates to the detection and management of the Steam Generator Tube Rupture (SGTR) faults and the incorporation of the design change proposed for the UK EPR™ during the later stages of GDA Step 4. My assessment has focussed on the deliverables identified within the EDF and AREVA Resolution Plans (Ref. 8) 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 Fault Studies Assessment identified a number of GDA Issues and Assessment Findings as part of the assessment of the evidence associated with the UK EPR™ reactor design. A GDA Issue is an observation of particular significance that requires resolution before ONR, an agency of HSE, would agree to the commencement of nuclear safety related construction of this reactor design within the UK. An Assessment Finding results from a lack of detailed information which has limited the extent of assessment and as a result additional information is required to underpin the assessment. However, they are to be carried forward as part of normal regulatory business during the site specific phase of the project as the detailed design develops.

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-FS-04**.

1.2 METHODOLOGY

5 My assessment has been undertaken in line with the requirements of the Office for Nuclear Regulation (ONR) HOW2 Business Management System (BMS) document AST/001 (Ref. 1) which sets down the process of assessment within ONR. The Safety Assessment Principles (SAPs), (Ref. 2), have been used as the basis for this assessment. Ultimately, the goal of assessment is to reach an independent and informed judgment on the adequacy of a nuclear safety case.

6 My assessment has 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.

7 The aim of my assessment is to provide a comprehensive review of the submissions provided in response to the GDA Issue to enable ONR to gain confidence that the concerns raised have been resolved sufficiently so that they can either be closed or less safety significant aspects be carried forward as Assessment Findings.

1.3 STRUCTURE

8 The Assessment Report structure differs slightly from the structure adopted for the previous reports produced within GDA, most notably the Step 4 Fault Studies Assessment at Ref. 7. Whilst previous reports have made extensive use of sampling, the present report builds on the previous work during GDA and focuses on the resolution of the GDA issues. As such this report is structured around the assessment of **GI-UKEPR-FS-04** rather than a report detailing close out of all GDA Issues associated with this technical topic area.

9 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 FAULT STUDIES – DESIGN BASIS FAULTS

10 The intended assessment strategy for GDA Close-out for the Fault Studies topic area was set out in a related assessment plan (Ref. 17) that identified the intended scope of the assessment and the standards and criteria that would be applied. This is summarised in the following Sections.

2.1 ASSESSMENT SCOPE

11 My report presents only the assessment undertaken as part of the resolution of the GDA Issue, **GI-UKEPR-FS-04**, relating the detection and management of the steam generator tube rupture faults (Ref. 6).

12 My report does not represent the complete assessment of UK EPR™ in the Fault Studies topic area for GDA and so it is recommend that this report be read in conjunction with the Step 4 Fault Studies Assessment (Ref. 7) of the EDF and AREVA UK EPR™ in order to appreciate the totality of the assessment of the evidence undertaken as part of the GDA process.

13 Similarly, my 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 Issues 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 the site specific phase. As such the possibility of further Assessment Findings being generated as a result of this assessment is not precluded.

14 The full text of the GDA Issue and Actions is provided in Annex 2. Reference 7 provides further background and explanatory information on the GDA Issue and Actions. EDF and AREVA have produced an individual Resolution Plan for the GDA Issue detailing the methods by which they intended to resolve the Issue through identified timescales and deliverables; see Reference 8.

15 A number of other assessment areas have provided input into the overall assessment of this Fault Studies GDA Issue. My report is consistent with those assessments. Where necessary, for example for more significant assessment items, this is reported in more detail elsewhere as referenced in the assessment section of this report (Section 4).

2.2 ASSESSMENT METHODOLOGY

16 My report has been prepared in accordance with relevant ONR guidance (Refs. 1 and 18) in coordination with the other assessment disciplines and the scope defined in the assessment plan (Ref. 6).

17 The assessment process consists of examining the evidence provided by EDF and AREVA in responding to the GDA Issue Actions. This is then assessed against the expectations and requirements of the SAPs and other guidance considered appropriate.

18 The basis of the assessment undertaken to prepare my report is therefore:

- Submissions made to ONR in accordance with the Resolution Plan.
- Updates to the Pre-construction Safety Report (PCSR) and its supporting documentation.

- The Design Reference that relates to the PCSR as set out in UK EPR™ GDA Project Instruction UKEPR-I-002 (Ref. 9) which has been updated throughout GDA Issue Resolution to include agreed design changes.
- Design Change Submissions – which are proposed by EDF and AREVA and submitted in accordance with UK-EPR GDA Project Instruction UKEPR-I-003, (Ref. 10).
- Consideration of internal and international standards and guidance, international experience, operational feedback and expertise and assessments performed by other regulators, especially their findings.
- Interaction with other relevant technical areas (where appropriate).
- Raising and issuing of Technical Queries (TQs) as appropriate, followed by assessment of Requesting Party (RP) responses.
- Holding necessary technical meetings to progress the identified lines of enquiry.

2.3 ASSESSMENT APPROACH

19 The approach to the closure of GDA for the UK EPR™ is described in greater detail in the Fault Studies assessment plan (Ref. 17) and is based upon the assessment methodology described above. The assessment covers the submissions made by EDF and AREVA in response to GDA Issues identified through the GDA process. These submissions are detailed within the EDF and AREVA Resolution Plans for each of the GDA Issues. The closure of each Fault Studies GDA Issue is reflected in a dedicated assessment report to describe the assessment process from the position established at the end of Step 4.

20 The overall strategy for closure of GDA is to build upon the assessment conducted during Step 4 and earlier, focussing on the detailed examination of the evidence presented by EDF and AREVA to support the satisfactory resolution of the GDA Issue Actions.

21 The following subsections provide an overview of the outcome from each of the information exchange mechanisms in further detail.

2.3.1 Technical Queries

22 I issued one Technical Query to EDF and AREVA relating to the management and mitigation of SGTR faults during close-out of **GI-UKEPR-FS-04** for UK EPR™ (Ref. 13).

23 I assessed EDF and AREVA's responses to this TQ as part of my assessment. Commentary on the most important and relevant TQ responses is included in the assessment section later in my report as appropriate. The responses provided by EDF and AREVA to these actions supplied further evidence supporting the overall judgement on the adequacy of resolution of the GDA Issues.

2.3.2 Technical Meetings

24 Provisions were made for a series of technical meetings with EDF and AREVA during assessment of the GDA Issue Action responses. These meetings occurred at appropriate points during 2011 and 2012 to monitor progress. These were supported by a number of teleconferences and smaller meetings, as necessary.

25 The principal focus of the meetings was to discuss progress and responses, to facilitate technical exchanges and to hold discussions with EDF and AREVA technical experts on emergent issues.

2.4 STANDARDS AND CRITERIA

26 Judgements have been made against the 2006 HSE Safety Assessment Principles (SAP) for Nuclear Facilities (Ref. 2). In particular, the fault analysis and design basis accident SAPs (FA.1 to FA.9), the severe accident SAPs (FA.15 to FA.16), the assurance of validity SAPs (FA.17 to FA.22), the numerical target SAPs (NT.1, Target 4, Target 7 to Target 9) and the engineering principles SAPs (EKP.2, EKP.3, EKP.5, EDR.1 to EDR.4, ESS.1, ESS.2, ESS.7 to ESS.9, ESS.11, ERC.1 to ERC.3) have been considered. The principle SAPs considered relevant to the close-out assessment are listed in Table 1. Other international guidelines such as Refs. 4 and 5 have also informed my assessment.

27 In addition, the following Technical Assessment Guides (TAG) have been used as part of this assessment (Ref. 3):

- T/AST/034 – Transient analysis for Design Basis Accidents in Nuclear Reactors.
- T/AST/042 – Validation of Computer Codes and Calculational Methods.

28 EDF and AREVA have assessed the safety case against their own design requirements.

2.5 USE OF TECHNICAL SUPPORT CONTRACTORS

29 It has not been necessary to employ the services of a Technical Support Contractor (TSC) as part of my assessment and resolution of this GDA Issue.

2.6 OUT-OF-SCOPE ITEMS

30 EDF and AREVA have added no items as out of scope to those identified during the GDA Step 4 assessment.

2.7 WORKING WITH OTHER REGULATORS

31 Interface with other international regulators has been principally by multilateral contact which has helped me to share the latest developments in this topic area. The contacts were enabled through Organisation for Economic Co-operation and Development (OECD) Nuclear Energy Agency (NEA) working group meetings in the context of the Multinational Design Evaluation Programme (MDEP) and other OECD ongoing NEA research working groups.

3 BACKGROUND TO THE GDA ISSUE AND EDF AND AREVA'S RESPONSES

3.1 OVERVIEW OF THE EDF AND AREVA SAFETY CASE FOR STEAM GENERATOR TUBE RUPTURE

32 An initial assessment of the Steam Generator Tube Rupture (SGTR) events during GDA Step 4 was undertaken as part of the faults leading to a decrease in the Reactor Coolant System (RCS) inventory (Ref. 7).

33 The inception and progression of a tube rupture within a steam generator (there are four on an EPR™) can be treated as small break that leads to depletion of the RCS inventory and depressurisation of the primary circuit, the magnitude of which depends on the break size. The loss of inventory is partly or fully compensated on the primary side by operational systems, in particular the Chemical and Volume Control System (CVCS). On the secondary side, the pressure remains stable and the affected SG (SGa) level increases depending on the capacity of the controllers to stabilize the plant, in particular the Main Feed Water System (MFWS) or the Start-up and Shutdown System (SSS), and the plant power level. Due to the transfer of radioactive coolant from the primary side into the affected SG, the activity sensors in the SG blowdown, the main steam lines and the condenser will detect a higher level of radioactivity than in normal operation.

34 Figure 1 identifies the simplified schematic locations of the proposed KRT radioactive detectors.

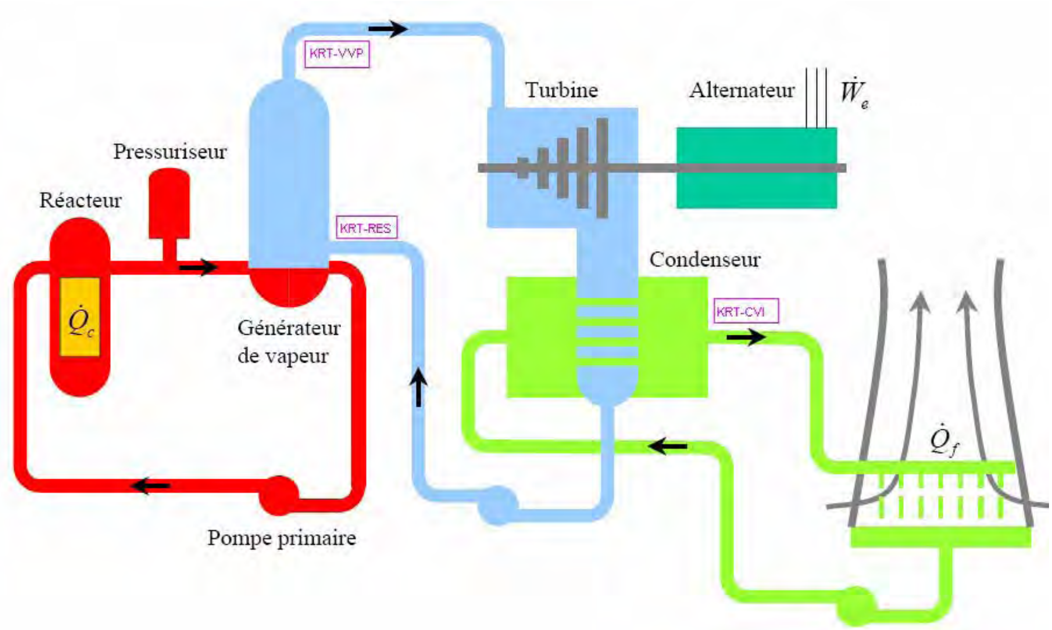

Figure 1. Simplified schematic view of the location of the radioactive KRT detectors

35 Two design basis SGTR faults are considered in the November 2009 PCSR (Ref. 11). The double-ended rupture of a single SG tube (2A-SGTR) identified as a, Plant Condition Category (PCC), PCC-3 design basis fault, and double-ended rupture of two SG tubes (4A-SGTR) that is identified as a PCC-4 design basis accident. The November 2009 PCSR claims a number of steam generator design features that have been included to reduce the probability of a SGTR event; including the choice of a ductile SG tube material,

the location of the blowdown system at the bottom of the SG tube bundle, chemistry control of the secondary water and activity control of the water on the secondary side within defined limits.

36 On initiation of an SGTR event, the continuous loss of RCS coolant inventory into the affected SG causes the pressuriser to empty. Significantly, the PCSR assumes that this results in a depressurisation of the RCS because the CVCS is not able to match the break flow (an assumption that is no longer supported, see below).

37 Upon the receipt of a Safety Injection (SI) signal on either low pressuriser pressure or high SG level from the affected SG, the UK EPR™ design causes a reactor trip and a deliberate partial cooldown of the RCS to lower the pressure sufficiently to allow injection from the Medium Head Safety Injection (MHSI) pumps, (further discussed in Ref. 7). The MHSI pumps are actuated following the safety injection signal but they do not inject until the primary pressure has dropped sufficiently (range 85 to 97 bara, Ref. 19).

38 EDF and AREVA propose that “controlled state” is reached when the MHSI injection and CVCS (if available) are able to match the SGTR flow rate. However, at this point the flow of primary coolant into the affected SG continues with potential activity release of contaminated water to the atmosphere. Additional discussion of “controlled state” is covered in Section 4.8.

39 From the controlled state, the affected SG is identified and isolated automatically. The isolation involves raising the Main Steam Relief Train (MSRT) setpoint above the MHSI shutoff head and closing the Main Steam Isolation Valve (MSIV). The isolation of the affected SG causes the flow via the break to increase the pressure in the affected SG. As the primary and secondary side pressures of the affected SG equalise, the flow via the break is gradually reduced and terminated.

40 This is defined as the end of the short term phase; a state which Ref. 11 claims can be achieved using only automatic Class 1 signals and systems. To achieve the safe shutdown[1], the operator is required to initiate boration via the Extra Boration System (EBS) and cooldown of the RCS using the unaffected SGs. It is the transition from the leak termination to safe shutdown that EDF and AREVA examine with the long term phase of the transient.

41 The claimed systems and operator actions required to transfer to the safe shutdown state were all at least Class 2 (F1B) (Ref. 11). No operator action was claimed before 30 minutes after the reactor trip. This was extended to one hour if local operator action was needed.

42 The description of the fault sequence following a SGTR event summarised above was assumed in Ref. 11 to be equally applicable for the PCC-3 single tube rupture and the PCC-4 two tube ruptures faults. However it was established during GDA Step 4 that the current UK EPR™ CVCS capacity is sufficient to compensate for a leakage up to more than a total guillotine break of a single SG tube. As a result, it was not possible to claim that a decrease of the RCS water inventory would be sufficient to trigger thermo-hydraulic protection signals. Similarly, the resulting increase in inventory in secondary side of the SGs could be compensated by a relatively small (~4%) reduction in MFWS flow when the plant is operated at full power. Therefore neither of the reactor trip signals on low

[1] The “safe shutdown state” is defined as a state where the affected SG is isolated and one of the Safety Injection System (SIS) or Residual Heat Removal System (RHRS) train is connected to the RCS.

pressuriser pressure or the high SG level could be assumed in the design basis safety case to be effective for the 2A-SGTR fault occurring at full power although, importantly, both would be available to automatically trip the reactor should either the CVCS or the feedwater control system fail to stabilise the reactor and SG water inventory.

43 This shortfall was discussed and recognised by EDF and AREVA during GDA Step 4, which lead to a programme of activity to modify the design and update the safety case. This modification is captured by Change Management Form at CMF #22 (Ref. 9) with a reliance on detection of increased secondary side activity levels to initiate operator action.

44 The UK EPR™ 2008 design freeze, which was assumed in the 2009 PCSR (Ref. 11), did have activity monitoring which could detect SG leakages. However, this was not credited in the design basis safety case. Detection of activity would be carried out at the steam outlet lines and on the SG blowdown line. It was originally proposed to have one N16 gamma detector per steam line. EDF and AREVA favour these detectors because of their sensitivity which allows relatively small leaks to be detected. However, they are larger than alternative designs (e.g. the detectors used on the SG blowdown line). Seismic limitations resulted in an original Class 3 (F2) safety classification for the activity monitoring system but EDF and AREVA have proposed to move the location of the SG blowdown water line detectors so that the system can be reclassified as Class 2 (F1B).

45 Claiming activity detection instead of the thermo-hydraulic protection systems, even after reclassifying the system to Class 2, did not meet EDF and AREVA's own design rules for PCC events needing Class 1 (F1A) systems to achieve the controlled state and leak termination. In Ref. 20, EDF and AREVA have considered two further design options to address this shortfall: providing a second N16 detector on the steam lines combined with a manual reactor trip or installing four NaI scintillator detectors on each steam line to provide an automatic trip with 2-out-of-4 voting logic. The intention was that either option will result in a reactor trip via Class 1 means. EDF and AREVA state that the N16 detectors are too large for four to be installed in the space available. This has lead to a favoured approach for the option of a manual reactor trip from two N16 detectors that could be positioned on the main steam line.

3.2 ASSESSMENT DURING GDA STEP 4

46 The Assessment of the UK EPR™ steam generator tube rupture safety case during Step 4 is reported in Ref. 7. This was principally based on the information made available to ONR on SGTR faults, which included the optioneering study of design changes to facilitate a trip on secondary side activity. However, Refs. 20 and 21 came in too late to be included in GDA Step 4 and only partially addressed the matters of concern to ONR. It was therefore judged that EDF and AREVA needed to take the complete design change (CMF #22), encompassing both the change in the physical design and the change to the safety case through the modification process, and a full impact assessment. This was therefore raised as a GDA Issue, **GI-UKEPR-FS-04,** Action 1.

47 EDF and AREVA (Ref. 20) have stated that their preferred strategy for mitigating a PCC-3 single SGTR fault is to claim a Class 1 (F1A) manual trip on activity detection and have presented arguments for the preference to utilise N16 detectors which are too large for 2-out-of-4 tripping logic. The larger detectors allow them to follow a management strategy based upon early detection of leaks that has been successfully adopted in the EDF French fleet, preventing the leaks from developing into the full 2A-tube ruptures. However, the arguments presented in Ref. 20 are restricted to the initial reactor trip.

48 In addition to a manual trip, the revised mitigation strategy also requires the operator to perform additional manual actions; such as, isolation of the affected SG and start of the Emergency Feed Water (EFW) to reach the controlled state. The equivalent actions in the original UK EPR™ design were all automatic. In the PCSR (Ref. 11) these additional actions are identified as Class 2 (F1B). It was therefore judged that from the evidence provided, the management of the PCC-3 SGTR fault did not meet EDF and AREVA's own design rule of relying on Class 1 (F1A) Systems, Structures and Components (SSC) to reach a controlled state and leak termination. As part of this work I therefore raised this matter as a GDA Issue, **GI-UKEPR-FS-04,** Action 2. In conjunction with Action 1 of this GDA Issue, EDF and AREVA were expected to provide more information on the safety classification of these manual actions and an ALARP argument to justify the proposed approach.

49 EDF and AREVA in Ref. 21 present new transient analysis of a single tube rupture assuming the manual trip and subsequent operator actions discussed above. Based on the information assessed during GDA Step 4, it was judged that EDF and AREVA should provide further substantiation of the operator actions to support the analysis provided. It was also noted that the operator actions of concern are all assumed to occur almost simultaneously 30 minutes after the break first opens. No justification for this was given and there is no discussion on whether failure to perform one of these actions successfully will change the fault sequence in a significant way. It may well be that failure of any particular action will prompt the series of automatic actions that were originally envisaged but no evidence for this had been provided. There was also no evidence that EDF and AREVA's examination of the limiting single failure remains valid with the revised strategy.

50 The analysis in the PCSR (Ref. 11) to demonstrate a margin to overfill and that the safe shutdown state can be reached for a single tube rupture considers a single transient occurring from 2% power without LOOP. The N16 detectors proposed are not claimed to be effective below 20% power, while measurements of SG secondary side pressure and level can still be claimed at low power. Therefore this analysis could potentially remain appropriate.

51 The assessment of the SGTR during GDA Step 4 concluded that whilst it is unlikely that the amount of radioactive steam that is released to atmosphere will change significantly, these differences will have an impact on the timing of key stages within the fault transient. It was therefore concluded that the reactor design has diverged from the analysis presented in the 2009 PCSR to such an extent that new analysis of the PCC-3 2A-SGTR event is required to demonstrate that there is a margin to overfill and that the long term safe shutdown state can be reached with safety criteria met. This is in line with the requirement of SAP FA.17 for theoretical models to adequately represent the facility, and SAP FA.7 which requires a conservative demonstration that adequate protection is provided. I raised the requirement to provide the revised fault analysis with assumptions appropriate for the UK EPR™ under GDA Issue **GI-UKEPR-FS-04,** Action 3.

52 In addition, the demonstration of a margin to overfill the SGa for the 4A-SGTR suffers from the same shortfalls as the equivalent analysis for the 2A-SGTR fault. It was therefore, concluded that the analysis presented does not reflect the UK EPR™ design sufficiently, so Action 3 of this GDA Issue also requires the reanalysis of the margin to overfill for the two tube rupture SGTR fault.

3.3 SUMMARY OF THE GDA ISSUE AND ACTIONS

53 GDA Issue **GI-UKEPR-FS-04** and its associated three Actions are given in Ref. 6. Further explanatory information on the resolution of this GDA Issue and Actions is provided in Ref. 8.

54 On the basis of the claims, arguments and evidence presented to the end of Step 4, it was considered that the UK EPR™ safety case related to SG tube rupture leak detection and managements required further work in three areas before the safety case can be regarded as satisfactory such that the GDA Issue could be closed.

55 The following provides the Actions associated with the GDA Issue **GI-UKEPR-FS-04** generated as a result of the Step 4 Fault Studies – Design Basis Faults Assessment that require EDF and AREVA to:

Action 1:

- Provide revised safety case and an ALARP argument to ONR to justify their proposed design to detect and mitigate PCC-3 Steam Generator Tube Ruptures faults.

Action 2:

- Provide detailed human factors justification of the actions claimed in the design basis safety case for the PCC-3 fault.

Action 3:

- Provide transient analysis to demonstrate that there is a margin to overfill for the design basis PCC-3 and PCC-4 SGTR faults, with assumptions appropriate for the UK EPR™.

56 The information provided by EDF and AREVA in response to this GDA Issue, as detailed within their Resolution Plan (Ref. 8), was broken down into the component GDA Issue Actions and then further broken down into specific deliverables for detailed assessment.

57 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 November 2009 PCSR (Ref. 11) which has already been subject to assessment during earlier stages of GDA. However, it is important to note that the deliverables essentially provide a revised safety case for the SGTR fault.

3.4 EDF AND AREVA DELIVERABLES IN RESPONSE TO THE GDA ISSUE ACTIONS

58 The published EDF and AREVA resolution plan for this Issue is given in Ref. 8. This provides details of the deliverables EDF and AREVA intended to provide to respond to the Actions listed. The following paragraphs contain a brief description of the deliverables supplied in response to each GDA Issue Action.

59 In Ref. 21, EDF and AREVA have reassessed the short term analysis of a single tube rupture from a pre-trip power of 102% (i.e. 4590 MWth) without LOOP assuming a manual trip prompted by secondary side Class 1 activity detection, 50 minutes after the break opens. The analysis covers time period between SGTR initiation and leak cancellation and credits a number of operator actions, including smooth power reduction, isolating the affected SG, raising the MSRT setpoint on the affected SG, stopping MFW flow to all SGs, disabling EFW flow to the affected SG and starting emergency feed water flow to the intact SGs. Ref. 21 predicts that 92 tonnes of steam will be discharged to atmosphere via the MSRT from the affected SG during the short term phase.

60 In addition, Ref. 21, presents a sensitivity study (Case 1) to demonstrate that following reactor trip, the engineered safeguard systems will automatically isolate the affected SG should the operator fail to do so.

61 This revised analysis predicted a rapid reduction in the water level within the affected SG after the main feed water has been isolated at 3000s. This leads to dry-out of the affected SG around 3500s after the start of the transient for a short period. The dry-out of the SG however, falls outside the EDF and AREVA's design basis assumption that no complete dry-out of the affected SG is anticipated during a postulated SGTR fault. EDF and AREVA therefore updated the procedures for recovery from a SGTR fault and reported the revised analysis in Ref. 22.

62 In Ref, 22, EDF and AREVA proposed to isolate the MSIV after partial cooldown is complete and they support this proposal by providing an analysis of a single tube rupture with plant parameters similar to that assumed in Ref. 21. The updated analysis examines the impact of implementing the revised operator intervention and predicts that the proposed procedures prevent the affected SG drying out with minimum water inventory of 26 tonnes remaining within the affected SG. Ref. 22 predicts a higher steam release of 218 tonnes discharged to atmosphere via the MSRT. The radioactive steam release via the affected SG during the transient are limited due to the isolation of the MSIV on the affected SG after the partial cooldown, with the bulk of steam discharge coming from other SGs.

63 The steam generator tube rupture mitigation strategy was updated at Ref. 23. The revised document builds upon the original strategy presented at Ref. 20, and considers the measures that can be implemented on the UK EPR™ design to reduce the radiological risk to the population to as low as reasonably practicable.

64 In Ref. 23, EDF and AREVA present the results of an optioneering study that includes the international operational experience feedback on SGTR events from existing Pressurised Water Reactors (PWR). The study acknowledges that in normal operating conditions, continuous leakage of RCS into the secondary side is allowed up to a predefined limit specified by the operating technical specification. EDF and AREVA (Ref. 23) however, argue that based on the international experience feedback (Ref. 24) and utilisation of the secondary side radiological sensors, the operators would be able to closely monitor the progression of the leak that may develop to a potential tube rupture and take the mitigation actions to limit the radiological releases to environment, as necessary.

65 EDF and AREVA have subsequently updated Sub-chapters 14.4 and 14.5 (Refs. 25 and 26) to include the impact of the results of revised analyses covering the PCC-3 and PCC-4 events. The resulting radiological consequences are presented in the relevant Sections of updated Sub-chapter 14.6 in Ref. 27.

4 ONR ASSESSMENT

66 Further to the assessment work undertaken during Step 4 (Ref. 7), and the resulting GDA Issue **GI-UKEPR-FS-04** (Ref. 6), my assessment focuses on substantiation of the approach adopted for the detection and management of the SGTR faults. Identified deliverables intended to provide the requisite evidence was provided within the responses contained within the Resolution Plan (Ref. 8) provided by EDF and AREVA at the end of Step 4 of GDA.

67 This assessment has been carried out in accordance with the ONR HOW2 document AST/001, "Assessment Process" (Ref. 1).

4.1 SCOPE OF ASSESSMENT UNDERTAKEN

68 The scope of the assessment has been to consider the expectations described in the GDA Issue, **GI-UKEPR-FS-04**, and the associated GDA Issue Actions. These are detailed within Annex 2 of this report. For each of the following areas further evidence was sought:

- A revised safety case including the ALARP argument to justify the proposed design to detect and mitigate PCC-3 SG tube ruptures faults.
- A detailed human factors justification of the actions claimed in the design basis safety case for the PCC-3 fault.
- Provision of transient analysis to demonstrate that there is a margin to overfill for the design basis PCC-3 and PCC-4 SGTR faults, with assumptions appropriate for the UK EPR™.

69 The scope of this assessment is neither to undertake further assessment of the PCSR nor 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 Fault Studies such that the existing safety case is undermined, these have been addressed.

4.2 ANALYSIS APPROACH

70 To examine the plant performance in SGTR fault covering the PCC-3 and PCC-4 events, the approach adopted by EDF and AREVA is to subdivide the transient into short term and long term phases to evaluate the reactivity release to the atmosphere for each phase separately. The short term phase is defined as up to the point of leak termination. This includes the controlled state in which the leak is compensated for by the RCS injection. In the long term phase, the plant is transferred to safe shutdown conditions with a possible activity release if depressurisation of the affected SG by the Main Steam Relief Train (MSRT) is required.

71 In the PCSR Sub-chapter 14.5 (Ref. 26), for the design basis fault covering PCC-4 sequences, a reactor trip is assumed to occur on either a low pressuriser level or high water SG level signal generated on the affected SG; depending on the initial state and operating conditions of the plant. The reactor trip automatically trips the turbine and the steam generator secondary side pressure rapidly increases. The Main Steam Bypass (MSB) to the condenser is assumed to be unavailable as it is not Class 1 safety system. This would also be unavailable following a Loss of Offsite Power (LOOP) occurring at the

time of turbine trip. Therefore, contaminated steam is assumed to be discharged to the atmosphere when the MSRTs are opened when the pressure setpoints are reached.

72 The continuous discharge of the primary coolant into the secondary side reduces the primary pressure and drains the pressuriser. The partial cooldown is initiated via the C&I controlled MSRT which will reduce the pressure in all the SGs. At the end of the RCS cooldown, the RCS pressure is higher than the Low Head Safety Injection (LHSI) maximum connecting pressure. To lower the pressure, the MSRT on the affected SG is opened. However, if the affected SG level is too high, the operator first opens the transfer line (a safety classified component of the SG blowdown route) between the affected SG and its partner SG to lower the level. This prevents overfilling the affected SG and considerably reduces the risk of an activity release to atmosphere.

73 Following isolation of the affected SG by closure of the MSRT and MSIV, the continuing break flow into the secondary side results in an increase in the pressure and water level within the affected SG. This flow will gradually reduce the pressure differential between the primary and secondary side, effectively reducing the break flow to negligible values. This corresponds to the end of short term phase with a margin to overfill to protect against gross discharge of liquid to atmosphere.

74 To achieve the safe shutdown condition, the operator is required to initiate boration via the Extra Boration System (EBS) and cooldown of the RCS using the unaffected SGs. It is the transition from the leak termination to safe shutdown that EDF and AREVA examine with the long term phase of the transient. The operator has the ability of opening the link between the affected SG and its partner SG for the transfer of water inventory. This is to prevent liquid phase discharge from the affected SG to the atmosphere prior to the final depressurisation of the system and successful connection of the Residual Heat Removal (RHR) system.

75 In the PCSR Sub-chapter 14.4 (Ref. 25), for the design basis fault covering PCC-3 sequences, in addition to the Class 1 safety protection system, on detection of increased secondary side activity levels within the affected SG, the operator can initiate power decrease and take the necessary steps to isolate the affected SG. The supporting analysis presented in Ref. 23 examines the impact of the operator action with a 50 minutes delay after the detection of increased radiation levels. This delay includes 30 minutes for the first operator action and a further delay of 20 minutes for a power decrease. This time delay is extended to 60 minutes when local operator action is required.

76 The operator is expected to isolate the affected SG by manually isolating the EFW and MFW flow if not already activated by high SG level or secondary side radiation detection, and start the EFW flow to the intact SGs. The operator is also expected to manually isolate the MSIV and increase the MSRT set point if not already activated on SG pressure. The operator can then commence manual cooldown and reactor coolant boration. In the event of a manual reactor trip, the anticipated operator actions will be activated once the reactor trip has been established.

4.3 METHOD OF ANALYSIS

77 Transient analysis is presented in Refs. 25 and 26 for the short term and long term phases. Cases without LOOP from a pre-trip power of 102% have been undertaken to evaluate the maximum amount of activity released to the environment, and with LOOP from a pre-trip power of 2%, to demonstrate that no SG overfilling occurs (and therefore no liquid is released to the environment prior to leak termination).

78 The revised analysis covering the plant behaviour involving the failure of two tubes in one steam generator (4A-SGTR), classified as a PCC-4 event (Ref. 26), has been undertaken for an EPR™ design with constant 4,590 MWth (102%) core power until reactor trip occurs. The analyses for the short term and long terms phases of the two tube rupture have been performed principally by using the CATHARE code. This code is an advanced, two-fluid, thermal hydraulic computer code designed for use in realistic studies of accidents in PWRs. It provides a detailed representation of the primary and secondary side behaviour. This is the same code that is used for the analysis of LOCA faults and provides detailed model of the SG tube rupture flow and SG filling behaviour.

79 Some of the analyses supporting the safety submissions investigating a single SG tube failure in one steam generator (2A-SGTR) classified as PCC-3 event were undertaken with S-RELAP5, reported in Ref. 25. These analyses were performed using full core power of 4,900 MWth, which is no longer applicable to the UK EPR™. Where this value is used in the supporting analysis, the PCSR contains discussion on the applicability of prediction using the core power of 4,900 MWth to the UK EPR™.

80 Like CATHARE, S-RELAP5 is a well established thermal hydraulic code supported with a wealth of documentary evidence and test results. I have not assessed the validation of this code as part of GDA closure activity. It is also expected that in developing the site specific PCSR, the legacy S-RELAP5 analysis will be replaced with new CATHARE analysis.

81 The assessment of CATHARE code is considered within the GDA Step 4 Fault Studies Assessment Report, Section 4.2.8.9 of Ref. 7, therefore, I did not consider this aspect of the revised analysis within my assessment of this GDA Issue.

4.4 SGTR FAULTS - PCC-3 EVENTS

82 EDF and AREVA have stated that their preferred strategy for mitigating a PCC-3 single SG tube rupture fault is to claim a Class 1 manual trip on increased secondary side activity levels. In safety submissions as part of GDA Step 4, EDF and AREVA have presented (Ref. 20) arguments as to why they prefer to utilise N16 detectors. It is argued that these larger detectors allow the operators to follow a strategy of early leak detection and management that has been successfully adopted in the EDF French fleet, preventing leaks from developing into the full 2A-tube ruptures.

83 In support of the GDA Issue, EDF and AREVA have provided a design basis analysis for the UK EPR™ Reference Plant to examine the impact of manual reactor trip 50 minutes after the detection of increased radioactivity within the main steam line. This is supported by the operational experience presented; which has also been used to formulate the Emergency Operating Procedures (EOP) following SGTR faults to reach the controlled state. This analysis justifies the adequacy of the revised procedures and uses the UK specific design reference data as expected by the GDA Issue Action 1.

84 This analysis is supported by a number of sensitivity assessments to examine the influence of the operator action on the development of the transient, and to identify the

limiting case regarding the radiological consequences until the leak is gradually terminated.

85 The numerical dose targets needed to comply with the EPR™ safety objectives for "effective dose" and for "equivalent thyroid dose" for the PCC-3 and PCC-4 faults are presented in the PCSR (Ref. 27). The analysis in the PCSR presents effective dose values, for the notional limiting individual, which are significantly below these targets using the combined steam release masses from the short and long term transients calculated from 102% power with no LOOP (from the two tube rupture fault analysis which is unaffected by the greater CVCS charging capacity). It should be noted that the site specific PCSR is expected to review the validity of these assumptions for the UK EPR™ when site specific analysis is undertaken.

86 The GDA Step 4 assessment of the design basis analysis identified a number of key parameters that were considered within the supporting analysis of the generic EPR™ reactor design, and required that any revised analysis be updated to include the key parameters for the proposed UK EPR™ reactor design. The use of this data could consequently influence the outcome of the analysis relating to quantity of steam released to the environment, timing of the key events and potential loss of margin to overfill the SG. The revised analysis provided in support of the GDA Issue closure utilise the UK EPR™ specific key parameters covering:

- Reactor power.
- MHSI injection is assumed to have a delivery pressure appropriate to the reactor power of 4,500 MWth design.
- The CVCS charging flow is updated to be 28 kg/s identified as the charging flow capacity of two pumps at the beginning of the transient (more than the break flow from a 2A-SGTR).
- Automatic isolation of the CVCS charging line following the combination of SG level and completion of partial cooldown signals.
- The low-low pressure signal activates the safety injection system and initiates an automatic partial cooldown rate of 250°C/h is assumed.
- The MSIV of all SGs are closed on the low SG pressure signal due to the depressurisation caused by blowdown of the affected SG. This operation can be performed manually, if necessary, after partial cooldown is finished.

87 EDF and AREVA only provided the steam generator tube rupture strategy (Ref. 20) during the later stages of Step 4 GDA assessment of the UK EPR™. As a result, GDA Issue **GI-UKEPR-FS-04,** was raised for EDF and AREVA to present an updated version of this document (Ref. 21) in which the analysis were provided with the UK EPR™ assumptions and simulating the operator actions to bring the plant under control and stop the leak from the primary circuit to the secondary side.

88 The scope of this updated document relates only to the "short term" phase of SGTR events (i.e. break initiation to leak cancellation), with the "long term" phase (leak cancellation to shutdown) the same as that described in the 2009 PCSR. I therefore consider only those aspects relevant to this "short term" phase.

4.4.1 Steam Generator Dry-out

89 A relevant aspect, which directly contradicts the arguments presented during GDA Step 4 assessment, relates to the prediction of the steam generator dry-out in the revised analysis presented in Ref. 21. I note that during Step 4 GDA assessment of the UK EPR™, ONR queried in Refs. 30 and 13 whether dry-out of the SG was possible. ONR also asked EDF and AREVA to justify the assumption that the sequences considered are bounding from a chemistry point of view, and whether SGTR events could give rise to the SG dry-out in the design basis events. The concern here was that Iodine retention could be significantly reduced if dry-out of the steam generator occurred.

90 EDF and AREVA in their response stated that "*in general, no complete dry-out occurs during postulated design basis SGTR accidents. In order to make it possible for the affected steam generator to dry out, two additional failures would usually be necessary (e.g., stuck-open Main Steam Relief Isolation Valve (MSRIV) and stuck-open Main Steam Relief Control Valve* (*MSRCV) on the same steam generator), which would be a beyond design basis condition*." On this basis, colleagues from Reactor Chemistry discipline accepted the argument that dry-out of the affected SG was beyond design basis and did not need to be considered for UK EPR™. I also note in the Step 4 Reactor Chemistry report that assurance should be given that this condition is not reached for UK EPR™ when site specific analysis is undertaken.

91 However, the analyses presented in response to **GI-UKEPR-FS-04** do not seem to support this argument. Figure 9 of PEPR-F.10.1665. (Ref. 21), shows that the mass of liquid in the affected SG in the "base case" drops to almost zero shortly after the reactor trip and feed water isolation at 3,000 seconds. In TQ-EPR-1603, I raised a query relating to the SG dry-out and asked for a clarification of the operator action that may be leading to this behaviour. In response, EDF and AREVA explained that the SG dry-out in the revised analysis is caused by the difference in manual reactor trip between this calculation and those presented in Ref. 20.

92 In their response, EDF and AREVA also acknowledged that it was their design intention to prevent SG dry-out occurring for design basis accident and the predictions provided in Ref. 21 did not meet their own requirements for such event. EDF and AREVA therefore proposed to modify the procedures to avoid SG dry-out in SGTR events. These revised procedures include isolation of the MSIV after partial cooldown completion. In cases where the MSRCV is available, the MSIV isolation is actuated at the time of manual reactor trip. These revised procedures are aligned with the procedures developed and optimised on both the Taishan (TSN) and Olkiluoto 3 (OL3) EPR™ Nuclear Power Plant (NPP) projects. The calculation utilising the revised procedures are presented in Revision 3 of this document (Ref. 22) showing that implementing the revised procedures avoids the SG dry-out occurring.

93 The response to TQ-EPR-1603 also states that although principle actions have been identified, the complete procedure is yet to be finalised for UK EPR™. I have considered the EDF and AREVA's response to this TQ and believe that successful intervention initiated by the proposed operator action is likely to prevent SG dry-out occurring.

94 I therefore judge that additional information needs to be presented covering detailed aspects of the proposal, and additional development in the safety case is required during the site specific phase of the project as the detailed design develops. For this reason, I am raising Assessment Finding **AF-UKEPR-FS-86** for a future licensee to further develop and optimise the revised operator actions and procedures, and its implementation to prevent SG dry-out, minimising activity released in SGTR faults.

AF-UKEPR-FS-86: *The licensee shall complete the development work on the optimisation of operator actions claimed to prevent SG dry-out post SGTR faults. The revised proposal is required to fully consider the expectations of Emergency Operating Procedures (EOP) for the UK EPR™.*

Required timescale: Mechanical, Electrical and C&I Safety Systems, Structures and Components - Before Inactive Commissioning.

95 I also note that the conservative assumption applied by EDF and AREVA is that activity released during an SGTR event are bounded by the assumption that contaminated secondary coolant is released as entrained moisture within the steam releases to atmosphere. EDF and AREVA assume a fraction of either 1% or 0.25% moisture carry-over from the affected SG depending on the assumptions utilised or the methodology adopted to perform the analysis. This aspect and the methodology employed was assessed during GDA Step 4 as part of Reactor Chemistry assessment of the UK EPR™ reactor design (Ref. 30) which concluded that overall, a case based upon this approach could be made, provided wet reducing conditions could be shown to be maintained at all times, which led to **AF-UKEPR-RC-40**. This Assessment Finding requires the Licensee to update the safety analysis for SGTR events presented in the safety case to be a clear and consistent safety justification for such events, based upon a single set of underlying assumptions. The chemistry aspects of the safety analysis should be consistent with current experimental data and knowledge on iodine chemistry.

96 The Assessment Finding also requires the future licensee to clearly link the assumptions used to the supporting transient analysis and the behaviour of the plant systems and where bounding assumptions are used these should be demonstrably so. I would therefore look to satisfactory resolution of this Assessment Finding during the detailed design stage of the UK EPR™.

4.4.2 Diversity for Frequent SGTR Faults

97 EDF and AREVA acknowledge that single tube SGTR faults are frequent occurrences that are covered by PCC-3 faults, Ref. 12. ONR's expectation is that a diverse means of protection should be provided for each safety function as required by SAPs EDR.2, EDR.4, ESS.27 and ESS.19. I therefore consider that there is a need to demonstrate functional diversity for the following sequences:

- SGTR with Anticipated Transient Without Trip (ATWT) event due to failure of Rod Cluster Control Assemblies (RCCA) to insert;
- SGTR with ATWT event due to failure of Reactor Protection System (RPS) to trip the reactor;
- SGTR without activation of the MHSI;
- SGTR without partial cooldown;
- SGTR without MSIV isolation;
- SGTR without MSRT isolation;
- SGTR without feedwater isolation;
- SGTR without EFWS; and
- SGTR with failure of operator to perform manual actions.

98 In my judgement, the first and second sequences are already bounded by the, Risk Reduction Category (RRC), RRC-A analysis performed for the frequent Small Break Loss of Coolant Accident (SBLOCA) fault together with ATWT events. Loss of MHSI is less important for SGTR faults as the RCS pressure remains well above their injection head for a significant period of time and ultimately the operator can switch to LHSI to provide make-up and boration. The EBS can also be used for RCS boration. In response to TQ-EPR-1603 (Ref. 16), EDF and AREVA have provided transient analysis to demonstrate that failure of partial cooldown is protected by automatic CVCS isolation coupled with manual transfer of the contents of the affected SG to its partner SG. During Step 4 of GDA, EDF and AREVA provided an ALARP justification for not providing diverse MSIV isolation for SGTR faults while Chapter 16.4 of the PCSR presents transient analysis for the failure to isolate the MSRT valve. EDF and AREVA argue that the feed control valve actuated by the Safety Automation System (SAS) provides a diverse means of feedwater isolation, a claim that is further discussed in the **GI-UKEPR-FS-02** close out report (Ref. 32). Failure of the EFWS can probably be protected against using RCS cooldown and MHSI injection or feed and bleed.

99 Although the safety case makes claims on operator action to isolate the affected SG it is important to note that the first sensitivity study case reported in Ref. 22 demonstrates that following manual reactor trip, the Class 1 protection system is able to automatically isolate the affected SG, commence partial cooldown, and raise the MSRT opening set point above that of the MHSI injection head. This is a particularly strong aspect of the UK EPR™ safety case for SGTR faults and represents a significant safety improvement over the previous generation of PWRs. Should the operator fail to trip the reactor on either of the diverse alarms provided, the CVCS and SG feedwater control system will stabilise the reactor and SG inventory. Should either of these non Class 1 protection systems fail to operate correctly then the protection system will automatically trip the reactor on either low pressuriser pressure or high SG level.

100 While my judgement is that there is quite a robust safety case for frequent SGTR faults on the UK EPR™ reactor for the purpose of the GDA Issue closure; there is, nevertheless, a need for a future licensee to formally demonstrate within the safety case (updated PCSR) that adequate functional diversity is provided. For this reason, I am raising Assessment Finding **AF-UKEPR-FS-87** requiring a future licensee to provide such a demonstration in a relevant safety case.

> **AF-UKEPR-FS-87:** *The licensee shall demonstrate that diverse protection is provided for each safety function for frequent SGTR faults*.
>
> **Required timescale:** Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site.

4.5 SGTR FAULTS - PCC-4 EVENTS

101 The assessment performed during GDA Step 4 of the safety submissions relating to the SGTR faults concluded that the safety case and transient analysis presented in the PCSR (Ref. 11) for two tube ruptures in the same SG (4A-SGTR) from a reactor initially at full power and with LOOP remains appropriate. The loss of inventory through the break is beyond the capacity of the CVCS (two pumps charging capability in the UK EPR™ reactor design) and therefore a reactor trip will be triggered by low pressuriser pressure.

102 The 4A-SGTR analysis does not take into account partial cooldown rate of 250°C/h. However, EDF and AREVA have demonstrated that the effect of an increase in partial

cooldown rate is minimal on design basis SGTR analysis because the assumed single failure is the Main Steam Relief Control Valve (MSRCV) of the affected SG stuck open. The steam flow from the failed open MSRCV is so great that cooldown is accomplished using only the affected SG's MSRT. The actual cooldown rate exceeds both 100°C/h and 250°C/h for the first part of the partial cooldown phase and therefore the change in the required manual cool-down rate is not a significant parameter in the design basis analysis of the transient.

103 The revised analysis (Ref. 26) also includes the effect of worst single failure and preventive maintenance at full power and with Reactor Coolant Pumps (RCP) operating (this is a pessimistic assumption with no LOOP) to predict the steam release to environment from all SGs prior to affected SG isolation and final depressurisation phase. This analysis demonstrates that margin to overfill is maintained which will minimise liquid release to environment.

104 EDF and AREVA also report that at the end of manual cooldown, the differential pressure across the break fluctuates as the EFWS flow to the unaffected SGs switches on and off. This, in some cases, results in a small amount of backflow into the RCS, the magnitude of which is dependant on the availability of the RCPs (forced flow within the primary circuit limiting backflow into the RCS). EDF and AREVA argue that this small amount of backflow (approx. 2 – 5 tons depending on the case being studied) should not present a concern from the potential boron dilution via this route and any potential associated criticality. I do however note the assessment of the safety submissions in support of the GDA closure of heterogeneous boron dilution safety case **(GI-UKEPR-FS-01)** has raised Assessment Findings **AF-UKEPR-FS-30** and **AF-UKEPR-FS-31** (Ref. 29) that requires a future licensee to provide a revised PSA for external heterogeneous boron dilution faults; and formally demonstrate that the case meets the PCC analysis rules defined in the PCSR. Additional discussion on fault identification and potential failure mode that could generate a large unborated water slug that can enter the RCS and identification of countermeasures available to protect against each event is provided in Ref. 29.

105 I would therefore look to the future licensee to provide a satisfactory resolution of these Assessment Findings by providing the relevant PSA submissions to demonstrate that the case meets the PCC analysis rules during the future development of the detailed design and safety submissions for a UK EPR™.

4.6 SECONDARY ACTIVITY MONITORING AND DETECTION SYSTEM

106 The topic of improving the performance of the SGTR leak detection system for up to and including a guillotine failure of one SG tube was the subject of discussion with EDF and AREVA during GDA Step 4. EDF and AREVA acknowledge that to meet the requirement for primary detection of the design basis faults for PCC-3 events a redundant and suitably qualified Class 1 detection system is required. This approach corresponds with the expectation of SAPs FA.4, FA.8 and FA.9 requiring that Design Basis Analysis (DBA) should provide an input into the safety classification and the engineering requirements for SSCs performing a safety function, the limits and conditions for safe operations and the identification of requirements for operator actions. In order to improve the performance of the SGTR leak detection system for up to and including a guillotine failure of one SG tube, EDF and AREVA have proposed to modify the design of the KRT-VVP channels (Figure 1) by adding a second detection channel on the main steam line on each steam generator and have updated their safety submissions accordingly (Ref. 9). This approach

will allow for detection of increased radiological releases into the secondary side and isolation of the affected SG independently.

107 This modification is captured by a related Change Management Form (CMF #22) in Ref. 9 with a reliance on detection of increased secondary activity levels to initiate operator action. The proposed design change for the UK EPR™ includes:

- Provision of two redundant Class 1 detection channels on the main steam line on each steam generator. The proposal also includes modification of the Control and Instrumentation (C&I) to transfer information from a Class 1 safety system. These channels are also seismically qualified to meet the requirements of Class 1 safety systems. Although the layout constraints have prevented physical separation of these detectors, the analysis of hazards likely to impact on the availability of these detectors has indicated that close physical proximity is unlikely to impact the related system classification requirements.
- Change management form (CMF #22) also includes upgrading to Class 2 safety classification of the activity sampling devices (KRT/RES) which extract continuously from the individual blowdown lines for chemical analysis and activity detection. To improve the impact resilience of the updated equipment, it is proposed to move these to the Nuclear Auxiliary Building (NAB) to reduce the risk of damage from other equipment falling in a seismic event. These devices are suitably seismically qualified to meet the relevant classification requirements. It is also understood that the support systems have been upgraded to meet the revised safety classification.
- The design change also covers procedural changes to reflect the reliance placed on operator action to initiate a controlled cooldown and then a reactor trip in response to alarms from the N16 sensors indicating a SG tube leak for leak sizes up to one tube diameter failure.

108 This design provision will enable operator actions to initiate a controlled cooldown and reactor trip in response to alarms from the N16 sensors indicating a SG tube leak, for leak sizes up to one tube diameter.

109 Assessment performed during GDA Step 4 of the safety submissions relating to the SGTR faults recognised that (partially) removing the automatic protection for SGTR faults management in the design basis safety case returns the design to an approach similar to that employed in operating PWRs, which remains valid with the revised proposal for the operator intervention to bring the plant to a controlled state.

110 EDF and AREVA have provisionally identified a location for the two redundant KRT-VVP channels and acknowledge that due to layout constraints these redundant channels can not be physically separated. EDF and AREVA argue that the need for physical separation can be relaxed because of the analysis of the hazards likely to impact these channels have indicated that physical separation of redundant parts of this system is not necessary in order to meet the architecture requirements of Class 1 system.

111 In TQ-EPR-1603 (Ref. 13), I requested that EDF and AREVA provide the layout of the proposed component configuration and outline the measures taken to ensure that the redundant detection systems are located in an optimum manner within the space restriction. EDF and AREVA in their response have indicated that a feasibility assessment has been performed with the space constraints on the existing plant design. This feasibility study has shown that the additional sensor could be installed in the main steam line adjacent to the existing sensor. A suitable space envelope has been identified which may require re-positioning of the original sensor to accommodate the proposed second sensor.

112 EDF and AREVA also indicated that although the space envelope has been identified, the revised configuration has not been fully integrated into the detailed proposed design plant layout. EDF and AREVA have however performed an impact assessment to demonstrate that the safety role of this equipment can be performed within the space constraint.

113 In summary, I have assessed the arguments and the risks associated with incorporating a redundant Class 1 detection channel within the main steam line and upgrading to Class 2 safety classification of the diverse activity sampling devices in support of the strategy for leak detection and management in SGTR fault conditions. EDF and AREVA report that these detectors can continuously detect very small primary to secondary leaks and benefit from good operational experience feedback reliability, and I have accepted this argument. However, given the safety function of these detection channels and additional diverse detection enhancement that is offered by a reasonable segregation, I consider that the location of these sensors should be reviewed within the detailed design of the site specific phase of the project.

114 I therefore judge that additional information needs to be presented covering detailed aspects of the approach and additional development in the safety case is required during the detailed design phase as licensing progresses. For this reason, I am raising Assessment Finding **AF-UKEPR-FS-88** for a future licensee to demonstrate that the location of these detectors are optimised to maximise their sensitivity for detecting any activity released from the primary to secondary side in SGTR faults.

> **AF-UKEPR-FS-88:** *The licensee shall provide a robust justification that the position of the steam line activity sensors is optimised to maximise their sensitivity for detecting the activity released from SGTR faults or to minimise potential radiological discharge to atmosphere*.
>
> **Required timescale:** Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to site.

4.7 RADIOLOGICAL CONSEQUENCES

115 The radiological consequences analysis presented in the revised PCSR Sub-Chapter 14.6 (Ref. 27) covering the 4A-SGTR (PCC-4) faults analysis are calculated from 102% power and with LOOP. These analyses take into consideration the new CVCS assumptions and are reported not to have any impact on the radiological assessment.

116 In addition, the radiological consequences analysis presented in the revised PCSR Sub-Chapter 14.6 (Ref. 27) covers the 2A-SGTR (PCC-3) fault using the revised plant conditions. Both the short term and long term aspects of this calculation remain unaffected by the change in the parameter for this fault condition. The updated analysis also takes into account the revised considerations for PCC-3 events and it is predicted to have no impact on the radiological assessment. Therefore, as long as the steam release assumed for this fault continues to bound that predicted for all other SGTR faults, the thermal hydraulic input assumptions in the radiological consequences analysis should remain valid.

117 I have therefore not undertaken any further assessment of the radiological consequences or potential consequential SGTR failures (e.g. due to steam line failure) as part the closure of this GDA Issue.

4.8 CONTROLLED STATE

118 EDF and AREVA in Ref. 22 propose that "controlled state" is reached when the core is subcritical and safety injection, if available and CVCS flow are able to match the SGTR flow rate. However, at this point the flow of primary coolant into the affected SG continues with potential activity release of contaminated water to the atmosphere. I acknowledge that the point of "controlled state" (as currently defined) is covered by the "short-term" analysis presented in Ref. 22. Although the purpose of the "short-term" study is to quantify the maximum amount of fluid released to the atmosphere from the affected steam generator prior to leak cancellation; in my judgment, it is necessary to redefine the "controlled state" for an SGTR fault as the time when the leak of primary coolant into the secondary side has diminished. On establishing this condition, the operator has managed to reduce the consequential risk of further discharges into the atmosphere and reduced the primary circuit pressure in a controlled manner.

119 I therefore judge that additional information needs to be presented covering detailed aspects of the approach to achieving a "controlled state" requiring Class 1 safety protection systems in the safety case during the detailed design phase as the site specific phase progresses. For this reason, I am raising Assessment Finding **AF-UKEPR-FS-89** for a future licensee to revise the definition of the "controlled state" to correspond with the completion of actions that lead to diminished flow from the primary to the secondary side to minimise any activity released into the atmosphere in SGTR faults. This will be required to ensure that only Class 1 safety protection systems are claimed for minimising the potential discharge to atmosphere.

> ***AF-UKEPR-FS-89:*** *The licensee shall review and update the definition of the "controlled state" for SGTR faults.*
>
> **Required timescale:** Mechanical, Electrical and C&I Safety Systems, Structures and Components – Before Delivery to Site.

120 The response to this Assessment Finding will need to feed into the response to a related Assessment Finding, **AF-UKEPR-CC-05,** which was raised as part of the cross-cutting GDA Step 4 report (Ref. 33) requiring a future licensee to apply the Safety Function (SF) and SSC methodologies identified in the GDA PCSR to the developing design for a UK EPR™ reactor.

4.9 HUMAN FACTORS

121 Action 2 of the GDA Issue **GI-UKEPR-FS-04** required EDF and AREVA to provide a human factors justification of the actions claimed in the design basis safety case for the PCC-3 fault. The related deterministic safety case (Ref. 22) for SG leaks (i.e. smaller than a single tube guillotine failure size) places a reliance on the operators to manually undertake a controlled cooldown and reactor trip within a 50 minute period.

122 EDF and AREVA have provided a detailed substantiation report (Ref. 31) for both the deterministic and probabilistic claims for operator responses to SGTR faults. This has followed the "Type C" methodology. Further information on this methodology and a summary of its assessment is provided in the GDA Closure report relating to GDA Issue **GI-UKEPR-HF-01** Identification and Substantiation of Human Based Safety Claims in Ref. 28.

123 The substantiation has identified that the manual cooldown and reactor trip appears feasible within the required timescale. However there are several issues that need to be addressed to ensure that the task is achieved reliably within the 50 minutes. These have

been recorded by EDF and AREVA in the Human Factors Issues Register (HFIR); specifically items 50-54 (see Ref. 31 for additional information) and cover:

- Consideration of task sequencing to ensure a manual Reactor Trip (RT) can be achieved earlier.
- Addressing various identified Human Machine Interface (HMI) details ensuring that there are sufficient HMI screens for the operator to use. One such generic case relates to the Operator Action (OA) problems with the number of screens available for showing desired Process Information and Control System (PICS) displays.
- Changing the power level for manual RT from 10% to 25% to ensure RT is undertaken earlier.
- Ensuring a clear and compelling cue when the power level drops to the required level for manual RT.

124 The full assessment of the HF submission (Ref. 31) has been performed by colleagues from the human factors discipline and reported in Ref. 28. It is judged that a manual cooldown leading to a manual reactor trip can be reliably achieved providing the issues identified by the HFIRs 50-54 are adequately addressed by a future licensee. This assessment has consequently concluded that EDF and AREVA have provided sufficient justification at this stage of design for the reliance on manual actions for the deterministic SGTR case as required by Action 2 of **GI-UKEPR-FS-04** on the basis that a future licensee will need to address the relevant HFIR issues (50-54).

125 In summary, I am satisfied that an adequate HF safety case has been submitted for the manual action to recover from an SGTR fault. I do however note the Assessment Finding **AF-UKEPR-HF-60** raised by the HF discipline in Ref. 28 that requires a future licensee to address and implement all the items identified from the GDA HF assessments and taken forward into the HFIR and Human Factors Assumptions Register (HFAR), or provide a justification as to any alternative position taken for any given item. A licensee should also provide ONR with a programme showing where and when in its future work it envisages addressing each HFIR item and assumptions.

126 I would therefore look to the future licensee to provide a satisfactory resolution of this Assessment Finding by providing a concise summary of key issues stemming from the HF safety case to address the future development of the detailed design and operating practices for a UK EPR™.

5 ASSESSMENT CONCLUSIONS

127 EDF and AREVA have undertaken a number of revised analyses work using UK EPR™ specific principal parameters within the Fault Studies assessment topic area during the close-out phase of GDA and have made significant progress in addressing the GDA Issue **GI-UKEPR-FS-04** on detection and management of SGTR faults identified by the GDA Step 4 assessment report.

128 In my opinion, EDF and AREVA have considerably strengthened the design basis safety case for the detection and management of SGTR faults for the UK EPR™ through the additional safety case information and revised analysis performed in response to GDA Issue **GI-UKEPR-FS-04**. This analysis has included provisions for operator intervention in tripping the reactor, depressurisation of the primary circuit and termination of leak from the primary side into the secondary. This is followed by procedures to isolate the SG to minimise the release of contaminated steam into the environment which has helped focus the comprehensive review of potential ALARP improvements. EDF and AREVA have performed a sensitivity analysis and updated the relevant sections of the safety case for the detection and management of the SGTR fault, where appropriate.

129 The analytical work performed by EDF and AREVA has been aided by important design changes to the detection systems on the UK EPR™ and also by some important changes in operating procedures that in my opinion will improve safety of the design. These changes have been proactively identified by EDF and AREVA to improve the performance of the SGTR leak detection system for up to and including a guillotine failure of one SG tube. The proposed design change for the UK EPR™ includes:

- Provision of two redundant Class 1 detection channels on the main steam line on each steam generator.
- Upgrading to Class 2 safety classification of the activity sampling devices which extracts continuously from the individual blowdown lines.
- Reliance on operator actions to initiate a controlled cooldown and reactor trip in response to alarms from the N16 sensors indicating a SG tube leak.
- Provision for the operator intervention to isolate the affected SG to prevent SG dry-out, and to limit the consequences of radiological release in the SGTR fault condition into the environment.

130 The human factors supporting analysis and review of operational experience has supported the claims made for manual intervention for SG tube leaks, although several changes to the detailed procedures have been identified to make the operator responses to SGTR faults more robust and reduce the likely time taken to manually trip the reactor. The HF submissions covering the changes in the operator actions required by the safety case are judged to have adequately justified the reliability of the claims being made.

131 EDF and AREVA have also updated the relevant section of the safety submissions to provide additional analyses demonstrating that there is margin to overfill the affected steam generator for the design basis PCC-3 and PCC-4 SGTR events using the UK specific plant data.

132 In my opinion, EDF and AREVA have performed a satisfactory review of the mitigation strategy aimed at demonstrating a reduction of the radiological risk from the SGTR faults and made significant progress in developing the detection and management strategy for the steam generator tube rupture faults.

5.1 OVERALL CONCLUSIONS

133 Overall, based on my assessment undertaken in accordance with ONR procedures, I am satisfied that the safety case for the detection and management of SGTR faults presented in the supporting documentation submitted in response to GDA Issue **GI-UKEPR-FS-04** is adequate subject to satisfactory progression and resolution of the Assessment Findings identified in Annex 2. These are to be addressed during the forward work programme for this reactor. For this reason, I am satisfied that GDA issue **GI-UKEPR-FS-04** can now be closed.

5.2 REVIEW OF THE UPDATE TO THE PCSR

134 Chapters 14.4 and 14.5 of the updated PCSR (Refs. 24 and 25) consider steam generator tube rupture (one Tube) and steam generator tube rupture (two Tubes in one SG) faults respectively. The impact of the revised analyses is covered in the relevant sections of the radiological consequences of design basis accidents presented in Chapter 14.6 (Ref. 26). These chapters were reviewed to ensure that the outcome of the GDA assessment had been appropriately captured within the PCSR. I am satisfied that the revised Chapters accurately reflect the analysis work and the proposed design modifications developed to justify the closure of **GI-UKEPR-FS-04**.

6 ASSESSMENT FINDINGS

135 The following Assessment Finding(s) have been raised:

AF-UKEPR-FS-86: *The licensee shall complete the development work on the optimisation of operator actions claimed to prevent SG dry-out post SGTR faults. The revised proposal is required to fully consider the expectations of Emergency Operating Procedures (EOP) for the UK EPR™.*

Required timescale: Mechanical, Electrical and C&I Safety Systems, Structures and Components - Before Inactive Commissioning.

AF-UKEPR-FS-87: *The licensee shall demonstrate that diverse protection is provided for each safety function for frequent SGTR faults*.

Required timescale: Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to Site.

AF-UKEPR-FS-88: *The licensee shall provide a robust justification that the position of the steam line activity sensors is optimised to maximise their sensitivity for detecting the activity released from SGTR faults or to minimise potential radiological discharge to atmosphere*.

Required timescale: Mechanical, Electrical and C&I Safety Systems, Structures and Components – delivery to site.

AF-UKEPR-FS-89: *The licensee shall review and update the definition of the "controlled state" for SGTR faults.*

Required timescale: Mechanical, Electrical and C&I Safety Systems, Structures and Components – Before Delivery to Site.

7 REFERENCES

1 *ONR HOW2 Business Management System. Assessment Process.* AST/001 Issue 4. HSE. April 2010. www.hse.gov.uk/nuclear/operational/assessment/index.htm.

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

3 Technical Assessment Guides:

Transient Analysis for Design Basis Accidents in Nuclear Reactors. T/AST/034 Issue 1. HSE. Nov 1999.

Validation of Computer Codes and Calculational Methods. T/AST/042 Issue 1. HSE. July 2000.

Structural Integrity Civil Engineering Aspects. T/AST/017 Issue 2. HSE. March 2005.

Probabilistic Safety Analysis.T/AST/030, Issue 3, HSE. Feb. 2009.

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

4 *Western European Nuclear Regulators' Association. Reactor Harmonization Group. WENRA Reactor Reference Safety Levels.* WENRA. January 2008. www.wenra.org.

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

6 *GDA Issue GI-UKEPR-FS-04 Revision 1, Steam Generator Tube Rupture Safety Case.* ONR. July 2011. TRIM Ref. 2011/361122, (TRIM folder 5.1.3.6348.).

7 *Step 4 Fault Studies – Design Basis Faults Assessment of the EDF and AREVA UK EPR™ Reactor*. ONR Assessment Report ONR-GDA-AR-11-020a Revision 0. TRIM Ref. 2010/581404, (TRIM folder 4.4.1.1827.).

8 *Resolution Plan for GDA Issue GI-UKEPR-FS-04 Revision 0.* EDF and AREVA. June 2011. TRIM Ref. 2011/336619. (in TRIM folder 5.1.3.6336.)

9 *Reference Design Configuration*. UKEPR-I-002, Revision 15. AREVA NP / EDF. 6 December 2012. TRIM Ref. 2012/478281.

10 *Design Change Procedure. UKEPR-I-003,* Revision 11. EDF and AREVA. 6 December 2012. TRIM Ref. 2012/478287.

11 *UK EPR Pre-construction Safety Report – November 2009 Submission.* Submitted under cover of letter UN REG EPR00226N. 30 November 2009. TRIM Ref. 2009/481363 and as detailed in UK EPR Submission Master List. November 2009. TRIM Ref. 2011/46364.

12 *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.

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

14 *Not Used.*

15 *Not Used*.

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

17 *Assessment Plan for fault Studies*. ONR-GDA-AP-11-007, Revision A, September 2011. TRIM Ref. 2011/479495.

18 *ONR HOW2 Business Management System Technical Reports.* AST/003 Issue 3. HSE. November 2009. www.hse.gov.uk/nuclear/operational/assessment/index.htm.

19 *EPR Sizing at 4500 MWth. EPRR DC 1685 Revision B*, AREVA, July 2002. TRIM Ref. 2011/134195.

20 *Steam Generator Tube Rupture Mitigation Strategy. PEPR-F DC 38 Revision A.* AREVA. December 2010. TRIM Ref. 2011/86029.

21 EPR™ *UK – GDA – GDA Issue FS04 – Update of Single Tube Steam Generator Tube Rupture Analysis for the UK EPR*. PEPR-F.10.1665. Rev. 2, AREVA, September 2011. TRIM Ref. 2011/494066.

22 EPR™ *UK – GDA – GDA Issue FS04 – Single Tube Steam Generator Tube Rupture Analysis for the UK EPR*. PEPR-F.10.1665. Rev. 3, AREVA, September 2012. TRIM Ref. 2012/369370.

23 *Steam Generator Tube Rupture Mitigation Strategy. PEPR-F DC 38 Revision D.* AREVA. October 2012. EPR01392N, TRIM Ref. 2012/386453.

24 *Monitoring reactor coolant/secondary side leaks for PWRs. D4550.15-11/0406, Rev. 1.* EDF. February 2011. EPR00800N, TRIM Ref. 2011/128768.

25 *PCSR – Sub-chapter 14.4 – Analyses of the PCC-3 events, UKEPR-0002-144, Issue 08,* November 2012. TRIM Ref. 2012/472432.

26 *PCSR – Sub-chapter 14.5 – Analyses of the PCC-4 events, UKEPR-0002-145, Issue 08,* November 2012. TRIM Ref. 2012/472433.

27 *PCSR – Sub-chapter 14.6 – Radiological consequences of design basis accidents, UKEPR-0002-146, Issue 06,* November 2012. TRIM Ref. 2012/472434.

28 *GDA Close-out for the EDF and AREVA UK EPR™ Reactor – GDA Issue GI-UKEPR-HF-01, – Identification & Substantiation of Human Based Safety Claims,* ONR Assessment Report ONR-GDA-AR-12-009a Revision 0. TRIM Ref. 2012/9, (TRIM folder 4.4.1.1931.).

29 *GDA Close-out for the EDF and AREVA UK EPR™ Reactor – GDA Issue GI-UKEPR-FS-01, – Heterogeneous Boron Dilution Safety Case,* ONR Assessment Report ONR-GDA-AR-12-010 Revision 0. TRIM Ref. 2012/10, (TRIM folder 4.4.1.1931.).

30 *Step 4 Reactor Chemistry Assessment of the EDF and AREVA UK EPR™ Reactor*. ONR Assessment Report ONR-GDA-AR-11-024, Revision 0. TRIM Ref. 2011/624477.

31 *PCSR Sub-Chapter 18.1 - Human Factors. UKEPR-0002-181, Issue 06*. November 2012, TRIM Ref. 2012/450490.

32 *GDA Close-out for the EDF and AREVA UK EPR™ Reactor – GDA Issue GI-UKEPR-FS-02, – Diversity for Frequent Faults,* ONR Assessment Report ONR-GDA-AR-12-011 Revision 0. TRIM Ref. 2012/11, (TRIM folder 4.4.1.1931.).

33 *Step 4 Cross-Cutting Topic Assessment of the EDF and AREVA UK EPR™ Reactor – Generic Design Assessment – New Civil Reactor Build,* ONR Assessment Report ONR-GDA-AR-11-032 Revision 0. TRIM Ref. 2010/581499, (TRIM folder 4.4.1.1827.).

Table 1

Relevant Safety Assessment Principles Considered for Close-out of GI-UKEPR-FS-04 Revision 0

SAP No.	SAP Title	Description
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.
ESS.19	Dedication to a single task	A safety system should be dedicated to the single task of performing its safety function.
ESS.24	Minimum operational equipment requirements	The minimum amount of operational safety system equipment for which any specified facility operation will be permitted should be defined and shown to meet the single failure criterion.
FA.17	Assurance of validity of data and models	Theoretical models should adequately represent the facility and site.
FA.4	Design Basis Analysis: Fault tolerance	DBA should be carried out to provide a robust demonstration of the fault tolerance of the engineering design and the effectiveness of the safety measures.
FA.7	Consequences	Analysis of design basis fault sequences should use appropriate tools and techniques, and be performed on a conservative basis to demonstrate that consequences are ALARP.

Table 1

Relevant Safety Assessment Principles Considered for Close-out of GI-UKEPR-FS-04 Revision 0

SAP No.	SAP Title	Description
FA.8	Design Basis Analysis: Linking of initiating faults, fault sequences and safety measures	DBA should provide a clear and auditable linking of initiating faults, fault sequences and safety measures.
FA.9	Design Basis Analysis: Further use of DBA	DBA should provide an input into the safety classification and the engineering requirements for systems, structures and components performing a safety function; the limits and conditions for safe operation; and the identification of requirements for operator actions.

Annex 1

GDA Assessment Findings Arising from GDA Close-out for GI-UKEPR-FS-04 Rev 1

Finding No.	Assessment Finding	MILESTONE (by which this item should be addressed)
AF-UKEPR-FS-86	Complete the development work on the optimisation of operator actions claimed to prevent SG dry-out post SGTR faults. The revised proposal is required to fully consider the expectations of Emergency Operating Procedures (EOP) for the UK EPR™.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – Before Inactive Commissioning
AF-UKEPR-FS-87	Demonstrate that diverse protection is provided for each safety function for frequent SGTR faults.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – Delivery to Site
AF-UKEPR-FS-88	Provide a robust justification that the position of the steam line activity sensors is optimised to maximise their sensitivity for detecting the activity released from SGTR faults or to minimise potential radiological discharge to atmosphere.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – Delivery to Site
AF-UKEPR-FS-89	Review and update the definition of the “controlled state” for SGTR faults.	Mechanical, Electrical and C&I Safety Systems, Structures and Components – Delivery to Site

…

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 <u>during</u> the operational phase. For other Assessment Findings, it is the regulators' expectation that the findings are adequately addressed no later than the milestones indicated above.

Annex 2

GDA Issue, GI-UKEPR-FS-04 Revision 1 – *Fault Studies – Design Basis Accidents* – UK EPR™

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

STEAM GENERATOR TUBE RUPTURE SAFETY CASE

GI-UKEPR-FS-04 REVISION 1

<table>
<tr><td colspan="2">Technical Area</td><td colspan="2">FAULT STUDIES</td></tr>
<tr><td colspan="2">Related Technical Areas</td><td colspan="2">Structural Integrity
Human Factors
Control and Instrumentation</td></tr>
<tr><td>GDA Issue Reference</td><td>GI-UKEPR-FS-04</td><td>GDA Issue Action Reference</td><td>GI-UKEPR-FS-04.A1</td></tr>
<tr><td>GDA Issue</td><td colspan="3">The safety case for steam generator tube rupture faults needs revising to incorporate significant design changes identified by EDF and AREVA. The safety case should demonstrate that the proposed detection and management strategy is ALARP and provide justification for the claims on operation actions. If the analysis shows that the proposed strategy is not ALARP, then alternative strategies will need to be developed.</td></tr>
<tr><td>GDA Issue Action</td><td colspan="3">EDF and AREVA to provide a revised safety case and an ALARP argument to ONR to justify their proposed design to detect and mitigate PCC-3 Steam Generator Tube Ruptures.

EDF and AREVA need to provide additional arguments and evidence to justify their design approach for PCC-3 SGTR faults or propose an alternative strategy. Therefore:
more information on the safety classification of these manual actions is required and an ALARP argument as to why they cannot be automated is to be provided, or
if an alternative strategy is identified, this similarly needs to be fully justified and substantiated, including new transient analysis.
Any proposed modification arising from the above is to be handled through the agreed process for managing design change in GDA.

EDF and AREVA shall update the PCSR and Fault Schedule in accordance with the agreed safety case.

With agreement from the Regulator this action may be completed by alternative means.</td></tr>
</table>

Annex 2

GDA Issue, GI-UKEPR-FS-04 Revision 1 – *Fault Studies – Design Basis Accidents* – UK EPR™

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

STEAM GENERATOR TUBE RUPTURE SAFETY CASE

GI-UKEPR-FS-04 REVISION 1

<table>
<tr><td colspan="2">Technical Area</td><td colspan="2">FAULT STUDIES</td></tr>
<tr><td colspan="2">Related Technical Areas</td><td colspan="2">Structural Integrity
Human Factors
Control and Instrumentation</td></tr>
<tr><td>GDA Issue Reference</td><td>GI-UKEPR-FS-04</td><td>GDA Issue Action Reference</td><td>GI-UKEPR-FS-04.A2</td></tr>
<tr><td>GDA Issue Action</td><td colspan="3">EDF and AREVA to provide a detailed human factors justification of the actions claimed in the design basis safety case for the PCC-3 fault.

In support of the ALARP case required in Action 1, a detailed human factors justification of any manual actions claimed in the design basis safety case for the PCC-3 fault is to be submitted to ONR-ND.

SGTR faults are amongst the most challenging events to ONR’s Target 4 for design basis fault sequences because of the potential for radioactive products to be discharged to atmosphere through the main steam relief train. EDF and AREVA have proposed a new mitigation strategy for the PCC-3 fault that departs from the typical UK EPR safety case principle of relying on automatic F1A (Class 1) actions to reach the controlled state. In addition to a manual reactor trip, the current proposals require the operator to perform additional manual actions such as isolation of the affected SG, start of the EFW.

With agreement from the Regulator this action may be completed by alternative means.</td></tr>
</table>

Annex 2

GDA Issue, GI-UKEPR-FS-04 Revision 1 – *Fault Studies – Design Basis Accidents* – UK EPR™

EDF AND AREVA UK EPR GENERIC DESIGN ASSESSMENT

GDA ISSUE

STEAM GENERATOR TUBE RUPTURE SAFETY CASE

GI-UKEPR-FS-04 REVISION 1

<table>
<tr><td colspan="2">Technical Area</td><td colspan="2">FAULT STUDIES</td></tr>
<tr><td colspan="2">Related Technical Areas</td><td colspan="2">Structural Integrity
Human Factors
Control and Instrumentation</td></tr>
<tr><td>GDA Issue Reference</td><td>GI-UKEPR-FS-04</td><td>GDA Issue Action Reference</td><td>GI-UKEPR-FS-04.A3</td></tr>
<tr><td>GDA Issue Action</td><td colspan="3">EDF and AREVA to provide transient analysis to show that there is a margin to overfill for the design basis PCC-3 and PCC-4 SGTR faults, with assumptions appropriate for the UK EPR.

The UK EPR design has diverged away from the analysis presented in the PCSR to such an extent that new analyses of the PCC-3 2A-SGTR and PCC-4 4A-SGTR events are required to demonstrate there is a margin to overfill and that the long term safe shutdown state can be reached with safety criteria met.

EDF and AREVA shall update the PCSR to reflect the revised analysis.

With agreement from the Regulator this action may be completed by alternative means.</td></tr>
</table>