HEALTH & SAFETY EXECUTIVE
NUCLEAR DIRECTORATE
ASSESSMENT REPORT

New Build

GDA Phase 1 - Step 2 EDF/AREVA – EPR Internal Hazard Assessment

HM Nuclear Installations Inspectorate
Redgrave Court
Merton Road
Bootle
Merseyside L20 7HS

1. INTRODUCTION

This assessment report records the Step 2 Internal Hazards assessment of the EDF/AREVA EPR submission in accordance with the strategy outlined in the Unit 6D operating plan, Ref 2.

Overall, it was concluded that the EDF/AREVA claims against the key Internal Hazard Safety Assessment Principles (SAPs) used in Step 2, were reasonable. Supporting arguments and evidence will be required, during Steps 3 & 4, to ensure that the EPR design complies with the claims and also complies, where reasonably practicable, with the full range of Internal Hazard SAPs.

In preparation for Step 3 the assessment made a number of observations which identified further information to be provided by EDF/AREVA in support of the claims.

2. ND ASSESSMENT

A proposal to licence new nuclear power stations in the UK is subjected to a two phase process as detailed in the Generic Design Assessment (GDA) – Guidance to Requesting Parties document, Ref 1. Phase 1 consists of 4 Steps and leads to the issuing of a Design Acceptance Confirmation. A Design Acceptance Confirmation means that the station design will be suitable for construction in the UK, subject to a site specific licence being granted at the completion of Phase two. This assessment report covers the Internal Hazard assessment carried out in Phase 1, Step 2. Phase 1, Step 2 of the GDA is called the "Fundamental Safety Overview" and covers an overview of the fundamental acceptability of the proposed design concept within the UK regulatory regime, Ref 1.

The overall assessment strategy for Step 2 is defined in the Unit 6D Operating Plan, Ref 2, and the specific Internal Hazard assessment strategy for Step 2 is given in ND Division 6 Assessment Report AR07010, Ref 3. As stated in the BMS guidance covering the NII assessment process, G/AST/001, Ref 4, "…..for a safety case to be effective it must provide three elements: *Claims, Evidence and Argument.*" The GDA addresses these elements in a stepwise approach. Phase 1, Step 2 addresses the claims. Phase 1, Step 3 addresses the arguments and Phase 1, Step 4 addresses the evidence. The completion of these Steps in Phase 1 constitutes the completion of the NII assessment covering the generic design and would lead to the issuing of the Design Acceptance Confirmation referred to above.

The objective of this assessment is therefore to consider whether EDF/AREVA claims that the relevant Internal Hazard SAPs are met. Assessment during Steps 3 & 4 will address the adequacy of the arguments and evidence supporting these claims respectively.

2.1 Requesting Parties Case

The EDF/AREVA Step 2 submission used during the assessment was located at S:\New Reactor Build\RP Submission\EDF_AREVA Submission 1 – Aug 2007. The submission was entitled, "UK-EPR Fundamental Safety Overview" (FSO).

Within the FSO submission EDF/AREVA did not provide a document that directly addressed compliance with each of the SAPs (e.g. a route map indicating the section(s) of the FSO that addressed each SAP). However, within the FSO, it was stated that, *"For this Fundamental Safety Overview submitted for Step 2 of pre-licensing, a systematic review of EPR safety features against UK requirements is not available. However, a limited review has been undertaken which indicates that the EPR design already meets the majority of UK requirements".* A Technical Query (TQ) – EPR000003 (Ref 5) was raised requesting an explanation of how the EPR design complied with each of the SAPs, including a request that EDF/AREVA provide an early response against the key Internal Hazard SAPs. EDF/AREVA's response to TQ EPR000003 (Ref 6), shows that EDF/AREVA claims compliance with the key Internal Hazards SAPs.

2.2 Standards and Criteria

The assessment is conducted in accordance with ND BMS procedures, AST/001, AST/002 and AST/003, Refs 8–10 respectively, and informed by the guidance given in the Internal Hazards Technical Assessment Guide (TAG) T/AST/014, Ref 11.

The Internal Hazard assessment strategy for Step 2 is given in ND DIV 6 Assessment Report AR07010, Ref 3. In accordance with this strategy, the Hazard SAPs, EHA.1 – EHA.17, Ref 7, were reviewed to identify key Internal Hazard SAPs that were relevant to the Step 2 assessment. To ensure that this selection covered an adequate set of Internal Hazard SAPs a further review was carried out against the WENRA reference levels, Ref 12, and the IAEA Nuclear Power Plant Design Requirements, Ref 13. The results of this review are shown in Annex 2 of the Internal Hazards assessment strategy, Ref 3, where they are ordered under assessment topics. These key Internal Hazard SAPs were used during the assessment.

2.3 ND Assessment

The definition of Internal Hazards is given in Ref 11, it states that, *"Internal hazards are those hazards to plant and structures such as fire, explosions, release of hazardous materials or gas, flooding etc, which originate within the site boundary, but external to the process in the case of nuclear chemical plant or primary circuit in the case of power reactors".* This definition was used in the assessment.

The key Internal Hazard assessment topics addressed in the assessment, as identified in the process described above, were:

- **Internal Hazards**
    - Identification
    - Operating Conditions
    - Analysis
    - Sources of Harm
    - Fire Detection and Fighting
    - Use of Material
- **Defence in Depth**
- **Layout**
    - Effects of Incidents
- **Safety Systems**
    - Failure Independence

The overall objective of these principles is to minimise the effects of internal hazards, particularly to ensure that internal hazards do not adversely affect the reliability of safety systems, designed to perform essential safety functions and that the potential common cause effects of internal hazards have been adequately addressed. Safety systems and safety related systems should be either qualified to withstand the effects of internal hazards or protected against the hazards, i.e. appropriate use of equipment qualification, redundancy, diversity, separation or segregation.

In achieving the objective, the principles require that a comprehensive and systematic approach is used to identify the internal hazards and that the hazards are then appropriately combined with consequential and/or simultaneous hazards and/or faults and, where necessary, take into account plant out for maintenance. A "defence in depth" approach should also be applied to internal hazards, for internal hazards that cannot be eliminated the following approach is used:

- Prevent the hazard
- Limit the severity of the hazard should it occur
- Limit the consequence of the hazard should it occur and be severe

The Step 2 assessment considered whether EDF/AREVA claimed that each key Internal Hazard SAP had been satisfied. The adequacy of any claim will be judged during STEPs 3 & 4 where the arguments and supporting evidence will be assessed. The assessment findings against the key Internal Hazard SAPs are presented in tabular form in Appendix 1. A summary, highlighting a number of observations to be considered during Step 3, is given below and should be read in conjunction with Appendix 1.

2.3.1 Internal hazards

EDF/AREVA claim that the EPR design complies with these SAPs, Ref 6.

In the response, Ref 6, EDF/AREVA referred to the following internal hazards: flood, missiles, pipe break, failure and leakage of pipes, tanks, pumps and valves, dropped loads, fire and explosion. The FSO includes details on how each internal hazard is being addressed within the design.

EDF/AREVA provide limited information on the methodology used to identify the hazards, it was therefore not possible at this Step, to judge whether all internal hazards had been adequately identified.

It was noted that the response, Ref 6, covering toxic gas release was treated as an external source (i.e. treated as an external hazard). However, there will be sources of the hazard arising from hazardous materials used and stored within the site boundary (an internal hazard). Consequently, in Step 2, it is not possible to confirm the completeness of the hazard listing.

Whilst EDF/AREVA claim compliance with SAPs EHA.1 & 14, supporting arguments will be required, during Step 3, to justify their claim and in particular the completeness of the hazard listing. The adequacy of the hazard identification methodology used will need to be assessed during Step 3 and tested using the additional hazards listed in Appendix 1 – EHA.1 & 14.

O1. Information will be required on the methodology used to identify internal hazards.

O2. Justification will be required for the completeness of the internal hazard listing.

The SAP requirement for hazard design basis faults should be assumed to occur simultaneously with the most adverse normal facility operating condition requires EDF/AREVA to define the condition. Although the SAP requirement covers both internal and external hazards, the EDF/AREVA response, Ref 6, only dealt with external hazards. A response covering internal hazards will be required in Step 3.

In claiming compliance with the SAP requirement, for the hazard analysis to include appropriate combinations of consequential and independent hazards and/or faults, EDF/AREVA referred to the FSO section dealing with the combination of external hazards and events. A response covering internal hazards will be required in Step 3.

Whilst EDF/AREVA claim compliance with EHA.5 & 6, supporting arguments will be required, during Step 3, to justify their claim and in particular that the EPR design has adequately addressed the internal hazard/fault combination requirements in EHA.5 & 6.

O3. Information will be required on the most adverse normal operating condition used in the internal hazards analysis.

O4. Information will be required on the specific combinations of internal hazards and faults included in the internal hazards analysis.

In the response, Ref 6, EDF/AREVA claim to provide fire detection and fire fighting devices to detect and fight a fire and to control it as quickly as possible.

Further statements in the FSO are made concerning the expected capacity and capability of the fire protection systems. These include:

"*Detection and fire fighting devices are installed to detect and fight the fire and to control the fire quickly as possible. The control requirements are as follows:*

- *The purpose of the detection system is to quickly detect the start of a fire, to locate the fire, to trigger an alarm and in some instances, to initiate automatic actions.*
- *The fire detection system must be operational in all cases where a fire is assumed to occur.*
- *Fire fighting devices, which are fixed or portable depending on the nature of the fire and the type of equipment to be protected, must be provided where a heat load is likely to generate a fire which could affect redundant equipment performing the same safety function."*

The last bullet point provides for the possibility that a fire protection system (fire detection and fire fighting system) could be employed to ensure that a safety system fulfils its safety function. This would imply that the fire protection system had a role in ensuring nuclear safety and would therefore require the allocation of an appropriate safety category and safety classification. This possibility is further supported by other statements in the FSO that provide for systems fulfilling F1 functions to be allocated to fire zones where the integrity of their border may be dependent on active fire protection devices. In order to confirm the appropriate safety categorisation and classification, EDF/AREVA should clarify the safety roles of the fire protection system.

It is noted that the design strategy in the majority of buildings, excluding the reactor building, is based on the provision of fire sectors which separate the systems and components important to safety with fire rated barriers. In some buildings, including the reactor building, an alternative design strategy is used which employs a combination of geographical separation, distance, thermal screens and fixed automatic protection (fixed and automatic fire fighting devices).

The fire resistance of safety related fire barriers is pre-defined, typically 2 hours. The adequacy of this fire rating is dependent on the combustibles in the fire sectors and the resulting fire severity. A justification for the fire resistance of the fire barriers is required.

In specifying a 2 hour fire resistance for a "Type 2 Safety Fire Sector", EDF/AREVA state, in the FSO, that in order to preserve the integrity of the fire barrier, that *"active and passive fire protection devices should be installed, where necessary, to ensure their integrity, in the event that the 2 hour resistance is exceeded."* Once again, this statement provides for the possibility that a fire protection system could be required to fulfil a safety role in preserving the "passive" defence to fire.

Finally, it is noted that the EDF/AREVA use of "geographical separation" to achieve formal segregation of redundant elements of the safety systems, is *"associated with an analysis which concludes that the time for the hot zone to reach all of the equipment is greater than the time required to extinguish the fire."* The dependency of the fire safety case on fire modelling will need to be identified, assessed and the fire models used supported by appropriate validation and verification studies.

Whilst EDF/AREVA claim compliance with SAP EHA.16, supporting arguments will be required, during Step 3, to justify their claim and in particular the adequacy of the fire barriers, the fire detection and fire fighting systems and any fire models.

O5. Justification will be required for the adequacy of the fire barriers. This should include: a justification of the fire severity and the fire barrier resistance, the designation of an appropriate safety categorisation and safety classification which reflects the barriers role with regard to safety and the measures for the control and design of penetrations.

O6. Justification will be required for the adequacy of the fire protection systems that are required to fulfil a safety role. This should include the designation of an appropriate safety categorisation and safety classification which reflects the systems role with regard to safety.

O7. The use of any fire models should be justified and include appropriate validation and verification studies.

O8. Justification will be required for any exceptions to the strategy of separating the redundant trains of safety related equipment with fire/hazard barriers.

2.3.2 Defence in Depth

EDF/AREVA claims that the EPR safety approach is based on the principle of defence in depth as prescribed in the IAEA Standard NS-R-1 "Safety of Nuclear Power Plants: Design."

It is noted that EDF/AREVA statements covering a number of internal hazards imply that the defence in depth philosophy is applied to the control and mitigation of internal hazards, most notably the fire hazard.

Whilst EDF/AREVA claims compliance with SAP EKP.3, supporting arguments will be required, during Step 3, to justify their claims and in particular the application of the defence in depth philosophy to all of the internal hazards.

O9. Information will be required on the application of the defence in depth philosophy (prevention, limiting severity and limiting consequences) to internal hazards.

2.3.3 Layout

EDF/AREVA refer to the layout provisions which are designed to minimise the effects of both internal and external hazards. The principle aim of these provisions is to minimise the impact of hazards on the safety systems. The scope of SAP ELO.4 also covers the provisions required to support access for any potential recovery actions following an event. EDF/AREVA confirm that any post recovery actions will be substantiated and based on written procedures and that a complementary specific assessment of access conditions will be conducted on a case by case basis. If post event actions are to be claimed then arguments and evidence will be required to justify them and particularly to justify the adequacy of any layout provisions, i.e. availability of access routes, emergency lighting etc.

Whilst EDF/AREVA claim compliance with SAP ELO.4, supporting arguments will be required, during Step 3, to justify their claim.

O10. Information will be required on the layout provisions required to facilitate access for any necessary recovery actions following an event.

2.3.4 Safety Systems

One of the requirements in SAP ESS.18 is to ensure that no internal hazard should disable a safety system. EDF/AREVA claim that the EPR has been designed such that the safety systems are physically separate, independent and isolated from other systems so that, following an internal hazard, the required safety functions are assured.

The FSO states that, *"If an internal hazard occurs in a "Type 1" building, the consequences of the hazard must be limited to the division affected. This means that the structures of the buildings necessary to prevent the propagation of the internal hazard (e.g. fire, high energy line break and flood) must be designed to withstand the consequences of the internal hazard."* The adequacy of these provisions is dependent upon the identification of all appropriate internal hazards and the specification of appropriate performance criteria for the passive "hazard" barriers which will be specific to the hazard challenge in their location, i.e. flood levels, missile impact, overpressure, fire severity, environmental effects etc.

Whilst EDF/AREVA claims compliance with the internal hazard aspects of SAP ESS.18, supporting arguments will be required, during Step 3, to justify their claim and in particular

the adequacy of the hazard barriers. This requirement is linked to the identification of internal hazards which has been discussed above, and the specification of the hazard challenge to each barrier or the equipment qualification.

O11. Justification will be required for the adequacy of the hazard barriers. This should include a justification of the hazard challenge to the barrier, a justification of the hazard barrier resistance, the designation of an appropriate safety categorisation and safety classification which reflects the barriers role with regard to safety and the measures for the control and design of penetrations.

2.3.5 General

The scope of the Step 2 assessment is limited to the key Internal Hazard SAPs. During Step 3 the full scope of the internal hazard and related SAPs will be assessed. Consequently, claims and supporting arguments will be required for the following SAPs:

O12. Claims and supporting arguments will be required for the remaining internal hazard and related SAPs, including:

EHA. 3, 4, 7, 10, 13 & 15

EHF.7

ESR.1 & 6

3. CONCLUSION

The Step 2 Internal Hazards assessment of the EPR was completed. The assessment in STEP2 considered the claims made by EDF/AREVA against each of the key Internal Hazard SAPs.

It was concluded that EDF/AREVA had made a claim against each key Internal Hazard SAP and as a consequence had met the assessment requirements of Step 2, Ref 2. Whilst the claims were judged to be reasonable, supporting arguments and evidence will be required, during STEPS 3 and 4, to confirm compliance with the claims and also to justify compliance, where reasonably practicable, with the full range of Internal Hazard SAPs. On that basis, I have no objection to the EPR proceeding to Step 3.

In preparation for Step 3 the assessment made a number of observations which identified further information to be provided by EDF/AREVA in support of the claims.

4. RECOMMENDATIONS

1. It is recommended that the observations identified throughout the assessment report should be raised with EDF/AREVA during Step 3.

5. REFERENCES

1. HSE Nuclear Power Station Generic Design Assessment – Guidance to Requesting Parties, Version 2, 16 July 2007.

2. HSE ND DIV 6 Unit 6D Operating Plan, 2 August 2007 – 31 March 2008.

3. HSE ND DIV 6 Assessment Report “GDA Phase 1 - Step 2 Internal Hazards Assessment Strategy”, Assessment Report No AR07010.

4. HSE ND – BMS G/AST/001, “Assessment Guidance – Assessment Process”, Issue 002, 28 February 2003.

5. Technical Query EPR000003 “Compliance with HSE Safety Assessment Principles for Nuclear Installations (2006 Edition).

6. EDF/AREVA response to Technical Query EPR000003, December 2007.

7. HSE Safety Assessment Principles for Nuclear Facilities, 2006 Edition.

8. HSE ND – BMS AST/001, “Assessment - Assessment Process”, Issue 002, 18 February 2003.

9. HSE, ND – BMS AST/002, “Assessment - Assessment Activity Management”, Issue 003, 16 April 2002.

10. HSE ND – BMS AST/003, “Assessment - Assessment Reporting”, Issue 002, 13 October 2003.

11. HSE ND – BMS, “Technical Assessment Guide – Internal Hazards”, T/AST/014, Issue 001, 24 June 1999.

12. Western European Nuclear Regulators Association (WENRA) Reactor Safety Reference Levels, January 2007.

13. IAEA Safety Standards Series – Safety of Nuclear Power Plants: Design – Requirements – No.NS-R-1.

APPENDIX 1

Assessment of Internal Hazard SAPs Considered During Step 2

Assessment Topic/SAP	Assessment
EXTERNAL AND INTERNAL HAZARDS	
Identification. *Principle EHA.1 - External and internal hazards that could affect the safety of the facility should be identified and treated as events that can give rise to possible initiating faults.* *Guidance – SAP paragraphs 211-213.* *211 This identification should include consequential events and, as appropriate, combinations of consequential events from a common initiating event.* *212 Any generic type of hazard with a total frequency that is demonstrably below once in ten million years may be excluded. Any generic type of hazard, the impact of which has no effect on the safety of the facility, can also be excluded. This screening should retain all hazards for which the frequency of realisation and the potential impact might make a significant contribution to the overall risks from the facility.* *213 The potential of a hazard to affect the safety of a facility may take account of factors such as the source of the hazard in relation to the facility and the design characteristics of the facility.*	EDF/AREVA claim that the *"EPR design is considered to comply with this principle."* The EDF/AREVA statement supporting this claim referred to several internal hazards, including flood, missiles, pipe break, failure and leakage of pipes, tanks, pumps and valves, dropped loads, fire and explosions and confirmed that internal hazards had been considered in the EPR design. The FSO documentation contains the following statements: *"The defence in depth approach requires that all internal and external hazards liable to affect reactor safety should be taken into consideration at the design stage."* and *"The defence-in-depth principle is also applied to the protection against internal events and hazards in order to limit their likelihood and consequences, through implementation of prevention, control and mitigation provisions. Design provisions are also made with respect to external hazards, consistent with provisions for internal events or hazards."* The statements acknowledge that internal hazards need to be identified and considered during the design phase. Limited information is included concerning the methodology used to identify the internal hazards. It is stated in the FSO that, *"The overall objective* [of the installation rules] *is to ensure that equipment required to carry out the three main safety functions* [core sub criticality, decay heat removal, radioactivity containment] *are suitably and adequately protected against the adverse effects of internal hazards"* and that *"an internal hazard must not adversely affect more than one element of a set of redundant F1 systems or prevent the systems carrying out the F1 functions."* It is clear that the overall objective of the EDF/AREVA internal hazards analysis is consistent with that of the SAPs; but that the approach is different. That is, EDF/AREVA do not necessarily treating an internal hazard as an initiating event, but treat them separately by assigning specific design objectives for the internal hazards. The adequacy of the supporting argument and evidence in justifying compliance with the objective of EHA.1 will need to be assessed during Steps 3 & 4. This assessment will need to consider the adequacy of the internal hazard identification process in identifying all credible internal hazards and should also include consideration of the following additional internal hazards: • Internal flooding arising from human error. • Spray effects from other than pipe failure, i.e. tanks, fire suppression systems, pump mechanical seals etc. • Spray effects of high energy pipe break. • Missiles arising from pipe breaks. • On-site transport. • Toxic and hazardous substances. • Overpressure from fires. • Fires due to transient combustibles.
Operating conditions	EDF/AREVA claim that the *"EPR design is considered to comply*

Assessment Topic/SAP	Assessment
Principle EHA.5 - Hazard design basis faults should be assumed to occur simultaneously with the most adverse normal facility operating condition.	*with this principle".* The EDF/AREVA statement supporting this claim did not address internal hazards. The FSO contains the following statement: *"The study* [internal hazards analysis] *is carried out for each of the buildings concerned, on the basis of rules similar to those used for initiating events (taking into account a single failure and plant unavailability due to preventive maintenance operations)."* The statement implies that the internal hazard analysis takes account of the unavailability of equipment including plant out for maintenance. The adequacy of the supporting argument and evidence in justifying compliance with EHA.5, particularly with respect to internal hazards and the required availability of safety related structures, systems and components, will need to be assessed during Steps 3 & 4.
Analysis *Principle EHA.6 - Analyses should take into account simultaneous effects, common cause failure, defence in depth and consequential effects.* *Guidance – SAP paragraph 217.* *217 To achieve the above two principles [EHA 5 & 6] the analysis should take into account that:* *a) certain internal or external hazards may not be independent of each other and may occur simultaneously or in a combination that it is reasonable to expect;* *b) an internal or external hazard may occur simultaneously with a facility fault, or when plant is out for maintenance;* *c) there is a significant potential for internal or external hazards to act as initiators of common cause failure, including loss of off-site power and other services;* *d) many internal and external hazards have the potential to threaten more than one level of defence in depth at once;* *e) internal hazards (e.g. fire) can arise as a consequence of faults internal or external to the site and should be included, therefore, in the relevant fault sequences; and* *f) the severity of the effects of the internal or external hazard experienced by the facility may be affected by facility layout, interaction, and building size and shape.*	EDF/AREVA claim that the *"EPR design is considered to comply with this principle".* The EDF/AREVA statement supporting this claim states that, *"Combinations of internal and external hazards are addressed in the EPR design."* However, the cross reference to the FSO for supporting information is limited to external hazards. Further information concerning internal hazards is required. The adequacy of the supporting argument and evidence in justifying compliance with EHA.6 will need to be assessed during Steps 3 & 4, with particular attention to appropriate combinations of internal hazards and faults in the analysis.
Fire, explosion, missiles, toxic gases etc – sources of harm *Principle EHA.14 – Sources that could give rise to fire, explosion, missiles, toxic gas release, collapsing or falling loads, pipe failure effects, or internal and external flooding should be identified, specified quantitatively and their potential as a source of harm to the nuclear facility assessed.* *Guidance – SAP paragraph 230.* *230 This identification should take into account:* *a) projects and planned future developments on and off*	EDF/AREVA claim that the *"EPR design is considered to comply with this principle".* The identification of internal hazards is addressed in the statements made against SAP principle EHA.1 above. HSE guidance covering the application of EHA.14 is given in SAP paragraph 230. It is noted that this paragraph increases the scope of EHA.14 with reference to incidents arising from on-site transport, on-site pipelines and on-site power and water supplies. The statements in the FSO do not make explicit reference to these potential hazards. Consequently, the adequacy of the supporting argument and

Assessment Topic/SAP	Assessment
the site; *b) the adequacy of protection of the nuclear facility from the effects of any incident in an installation, means of transport, pipeline, power supplies, water supplies etc either inside or outside the nuclear site.* *c) sources could be either on or off the site;*	evidence in justifying compliance with EHA.14, including the guidance, will need to be assessed during Steps 3 & 4.
Fire, explosion, missiles, toxic gases etc – fire detection and fighting *Principle EHA.16 – Fire detection and fire-fighting systems of a capacity and capability commensurate with the credible worst-case scenarios should be provided.* Guidance – SAP paragraphs 232-233. 232 The systems should be designed and located so that any damage they may sustain or their spurious operation does not affect the safety of the facility. 233 A fire hazard analysis should be made of the facility to: *a) analyse the potential for fire initiation and growth and the possible consequences on safety systems and other structures, systems and components important to safety;* *b) determine the need for segregation of plant and the location and required fire resistance of boundaries to limit the spread of fire; and* *c) determine the capacity and capability of the detection and fire-fighting systems to be provided.*	EDF/AREVA claim that the *"EPR design is considered to comply with this principle".* The EDF/AREVA statement supporting this claim states, *"Limiting the spread of a fire (containment) is achieved by dividing the buildings into fire compartments which use physical or geographical separation principles."* The supporting statement refers to the use of fire compartments and fire cells which, using the terminology on the FSO, are related to fire sectors and fire zones respectively. The FSO refers to the design basis of the fire protection systems. It is stated that, *"The design of the fire protection systems is based on three types of measures which are based on the three levels of in-depth protection (prevention, detection and extinguishing)."* The provision of fire detection and fire-fighting systems is an integral part of the overall fire protection strategy for the EPR. Further statements, in the FSO, are made concerning the expected capacity and capability of the fire protection systems. These include, "*Detection and fire fighting devices are installed to detect and fight the fire and to control the fire quickly as possible. The control requirements are as follows:* • *The purpose of the detection system is to quickly detect the start of a fire, to locate the fire, to trigger an alarm and in some instances, to initiate automatic actions.* • *The fire detection system must be operational in all cases where a fire is assumed to occur.* • *Fire fighting devices, which are fixed or portable depending on the nature of the fire and the type of equipment to be protected, must be provided where a heat load is likely to generate a fire which could affect redundant equipment performing the same safety function."* The adequacy of the supporting argument and evidence in justifying compliance with EHA.16 will need to be assessed during Steps 3 & 4, with particular attention to the: • Safety categorisation and classification of hazard barriers. • Justification of hazard barrier fire resistance. • Single failure tolerance of active penetrations in the hazard barriers, where appropriate. • Safety categorisation and classification of the fire protection system (Fire detection and fire fighting systems). • Justification of fire models. • Compliance with the relevant good practice established in the IAEA Safety Guide NS-G-1.7 "Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants."
Fire, explosion, missiles, toxic gases etc – use of material *Principle EHA.17 - Non-combustible or fire-retardant and heat-*	EDF/AREVA claim that the *"EPR design is considered to comply with this principle".*

Assessment Topic/SAP	Assessment
resistant materials should be used throughout the facility.	The EDF/AREVA statement supporting this claim refers to the "defence-in-depth" principle, particularly the fire prevention provisions. The FSO documentation supporting this claim commits, as part of the fire prevention strategy, to giving preference to the use of non-combustible materials. The adequacy of the supporting argument and evidence in justifying compliance with EHA.17 will need to be assessed during Steps 3 & 4, with particular attention to the definition and standards used to determine non-combustibility.
KEY PRINCIPLES	
Defence in depth *Principle EKP.3 - A nuclear facility should be so designed and operated that defence in depth against potentially significant faults or failures is achieved by the provision of several levels of protection.* *Guidance – SAP paragraphs 140-144 & Table 1 (not included)* *140 International consensus is that the appropriate strategy for achieving the overall safety objective is through the application of the concept of defence in depth. This should provide a series of levels of defence (inherent features, equipment and procedures) aimed at preventing accidents and ensuring appropriate protection in the event that prevention fails.* *141 The levels of protection should prevent faults, or if prevention fails should ensure detection, limit the potential consequences and prevent escalation.* *142 The concept of defence in depth should be applied so that:* *a) deviations from normal operation and failures of structures, systems and components important to safety are prevented;* *b) any deviations from normal operation are allowed for by safety margins that enable detection and action that prevents escalation;* *c) inherent safety features of the facility, fail-safe design and safety measures are provided to prevent fault conditions that occur from progressing to accidents;* *d) additional measures are provided to mitigate the consequences of severe accidents.* *143 Defence in depth is generally applied in five levels. The methodology ensures that if one level fails, it will be compensated for, or corrected by, the subsequent level. The aims for each level of protection are described in detail in IAEA Safety Standard NS-R-1, on which Table 1 is based. It should be noted that Table 1 deals with the application of defence in depth in the design of a facility, and does not deal with other important contributions such as human performance or equipment reliability. These topics are addressed in other sections of the SAPs.* *144 An important aspect of the implementation of defence in depth is the provision of multiple, and as far as possible independent, barriers to the release of radioactive substances to the environment, and to ensure the confinement of radioactive*	EDF/AREVA claim that the *"EPR design is considered to comply with this principle".* The EDF/AREVA statement supporting this claim refers to compliance with the defence in depth requirements in the IAEA Standard NS-R-1. The FSO documentation supporting this claim contains the following statements: *"Implementation of the defence-in-depth approach is required. The concept is based on a series of levels of defence, the first four of which are taken into account in the design. These are:* • *first level of defence: combination of conservative design, quality assurance, high quality of fabrication and high level of surveillance activities (controls, monitoring) to prevent departures from normal plant operation.* • *second level of defence: detection and control of abnormal operating conditions in order to prevent accidents. Specific attention is paid to ensuring the integrity of the fuel cladding and the Reactor Coolant Pressure Boundary (RCPB).* • *third level of defence: control of accidents and prevention of severe accidents (core melt accidents). Design features and systems are provided to mitigate accidents.* • *fourth level of defence: measures to preserve the integrity of the containment and to control severe accidents.* • *The fifth level of defence is provided by measures for emergency control and on- and off-site emergency response. This is not directly linked with the generic design of the plant."* In addition, the FSO documentation also states that: *"The defence in depth principle is applied to the protection against internal events and hazards in order to limit their likelihood and consequences, through the implementation of prevention, control & mitigation measures".* The adequacy of the supporting argument and evidence in justifying compliance with EKP.3 will need to be assessed during Steps 3 & 4.

Assessment Topic/SAP	Assessment
substances at specified locations. The number of barriers will depend on the magnitude of the radiological hazard and the consequences of failure.	
LAYOUT	
Minimisation of the effects of incidents *Principle ELO.4 - The design and layout of the site and its facilities, the plant within a facility and support facilities and services should be such that the effects of incidents are minimised.* *Guidance – SAP paragraphs 206-207.* *206 For example, the design and layout should:* *a) minimise the direct effects of incidents, particularly internal and external hazards, on structures, systems or components;* *b) minimise any interactions between a failed structure, system or component and other safety-related structures, systems or components;* *c) ensure site personnel are physically protected from direct or indirect effects of incidents;* *d) facilitate access for necessary recovery actions following an event.* *207 Support facilities and services important to the safe operation of the nuclear facility should be designed and routed so that, in the event of incidents, sufficient capability to perform their emergency functions will remain. Support facilities and services include access roads, water supplies, fire mains and site communications.*	EDF/AREVA claim that the *"EPR design is considered to comply with the SAP".* The EDF/AREVA statement supporting this claim refers to the layout provisions which are designed to minimise the effects of both internal and external hazards. The principle aim of these provisions is to minimise the impact of hazards on the safety systems. The scope of SAP ELO.4 also covers the provisions required to support access for any recovery actions following an event. EDF/AREVA confirm that any post recovery actions will be substantiated and based on written procedures and that a complementary specific assessment of access conditions will be conducted on a case by case basis. The "Fundamental Safety Overview" documentation supporting this claim contains the following statements: *"Protection against internal hazards must* [be] *considered in the design of the unit, through layout requirements and/or design against hazard loads. If an internal hazard occurs in a type 1 building* [building separated into divisions], *the hazard must be limited to the division affected. If an internal hazard occurs in a type 2 building* [building not separated into divisions], *the installation rules or the design must ensure that not more than one redundant F1 system is affected."* The "Fundamental Safety Overview" documentation supporting this claim also recognises the need to minimise the effects of internal hazards on appropriate personnel and states that: *"Design measures are taken into consideration to ensure the protection and safe egress of occupants……"* and *"Individual fire areas are established to confine fires to their area of origin and to prevent fires from spreading to adjacent fire areas. A fire area designated "Access Area" is defined to protect the means of egress of plant personnel and access for the fire brigade."* The objective of this design philosophy is to minimise the effects of the internal hazards. The adequacy of the supporting argument and evidence in justifying compliance with ELO.4 will need to be assessed during Steps 3 & 4.
SAFETY SYSTEMS	
Failure Independence *Principle ESS.18 - No fault, internal or external hazard should disable a safety system.* *Guidance – SAP paragraph 352.* *352 Safety systems should be physically separate, independent, isolated from other systems, including safety-related systems, and share no equipment or services. There should be adequate segregation between independent parts of the safety system (including pipework and cabling) and also between a safety system and other facility equipment that, in the event of a fault, might jeopardise the safe working of the safety system.*	EDF/AREVA claim that the *"EPR design is considered to comply with this principle".* The EDF/AREVA statement supporting this claim refers to the EPR safety systems being physically separate, independent and isolated from other systems. The FSO documentation supporting this claim contains the following statements: *"The main safeguards are arranged in a four-train configuration. The 4 trains are physically separated. Physical separation reduces the risks of dependent failures between redundant trains, in particular those that could result from internal hazards. The architecture makes it possible for a system to fulfil its safety function even if one train is affected by a single failure while*

Assessment Topic/SAP	Assessment
	another train is unavailable due to a preventative maintenance." This deterministic design philosophy aims to ensure that an internal hazard will not prevent a safety system fulfilling its safety function. The adequacy of the supporting argument and evidence in justifying compliance with ESS.18 will need to be assessed during Steps 3 & 4.