UK EPR	Title: PCSR – Sub-chapter 3.1 – General Safety Principles
	UKEPR-0002-031 Issue 04

Total number of pages: 54	Page No.: I / IV
Chapter Pilot: M. BERNARD *Name/Initials* *Date 31-10-2012*	
Approved for EDF by: A. MARECHAL *Name/Initials* A.Je.Marechal *Date 08-11-2012*	Approved for AREVA by: G. CRAIG *Name/Initials* G Craig *Date 08-11-2012*

REVISION HISTORY

Issue	Description	Date
00	First issue for INSA review	14.01.08
01	Integration of co-applicant and INSA review comments	29-04-08
02	PCSR June 2009 update: – Clarification of text – Integration of references – Erratum corrections – Section 1.2.3.5.2: definition of internal hazards extended to include hazards occurring outside buildings which are a threat to nuclear safety. – Section 1.2.3.6 added referring to fault and protection schedule – Table 1 amended to official English version of the Technical Guidelines	25-06-09
03	Consolidated Step 4 PCSR update: – Minor editorial changes – Update of PCSR cross-references – Sections 1.2.1.4.1, 1.2.1.4.2, 1.2.3.5.2: Introduction of High Integrity Component (HIC) claim – Section 1.2.3.5: outline of hazards methodology added, including the link between PCC/RRC ("internal faults") and hazards – Section 1.2.5: Update of text consistent with Sub-chapter 3.2 – Figure 6 updated (consistent with Sub-chapter 3.2); Figures 7A, 7B and 7C removed	27-03-11

Continued on next page

REVISION HISTORY (Cont'd)

Issue	Description	Date
04	Consolidated PCSR update: - References listed under each numbered section or sub-section heading numbered [Ref-1], [Ref-2], [Ref-3], etc - Minor editorial changes - Section 1.2.1.4: update of High Integrity Component (HIC) regarding break preclusion, addition of Main Steam Isolation Valve (MSIV) - Section 1.2.2.4: complete update of sub-section "Human Factors" - Section 1.2.5: update of text consistent with Sub-chapter 3.2 - Section 2.2: addition of information regarding applicability of technical guidelines - Reference for Technical Guidelines in §1.2, §1.2.4.2, §2.1 moved to Table 1; content of Table 1 deleted and replaced by reference with a caveat regarding the applicability to the UK context. - Figure 6 removed (already provided in a new version in Sub-chapter 3.2)	08-11-2012

For information address:

AREVA NP SAS
Tour AREVA
92084 Paris La Défense Cedex
France

EDF
Division Ingéniérie Nucléaire
Centre National d'Equipement Nucléaire
165-173, avenue Pierre Brossolette
BP900
92542 Montrouge
France

TABLE OF CONTENTS

SUB-CHAPTER 3.1 – GENERAL SAFETY PRINCIPLES

1. OBJECTIVES AND SAFETY PRINCIPLES

1.1. INTRODUCTION

1.1.1. Overview

This sub-chapter describes the safety approach implemented in the EPR plant design.

It provides both a summary of the main EPR design requirements and a description of the main technical approach adopted to meet these requirements. It points to other chapters in this PCSR in which safety requirements applicable to the topics dealt with are set out in more detail.

Although the sub-chapter is concerned mainly with design principles adopted to meet requirements of the French Safety Authority, reference is also made to supplementary safety design requirements that would be demonstrated for an EPR operating in the UK to address UK specific safety principles.

1.1.2. Overall objectives

The EPR is a Generation 3+ reactor and benefits through its evolutionary design from global international experience acquired at both PWR system operational level in western countries, and French and German engineering design experience.

The safety approach at the design level is based on the concept of defence in depth which involves a stratified layering of provisions (or lines of defence) to mitigate the effects of technical or human failures.

As presented internationally, (see for example IAEA standard NS-R-1 [Ref-1]), defence in depth generally has a 5-level structure:

- Level 1 is a combination of design, quality assurance and control margins aimed at preventing the occurrence of abnormal operating conditions or plant failures,
- Level 2 consists of the implementation of protection devices which make it possible to detect and correct the effects of deviations from normal operation or the effects of system failures. This defence level is aimed at ensuring the integrity of fuel cladding and that of the primary cooling system so as to prevent accidents,
- Level 3 consists of safeguard systems, protection devices and operating procedures which make it possible to control the consequences of accidents that may occur so as to contain radioactive material and prevent the occurrence of severe accidents,
- Level 4 comprises measures aimed at preserving containment integrity and controlling severe accidents,
- Level 5 includes, in the event of the failure of previous levels of defence, all measures for protecting the public against the effects of significant radiological releases. Such measures for emergency control and on- and off-site emergency response are not directly linked with the generic design of a plant.

Attaining a significantly superior safety level for the EPR reactor is achieved, on the one hand, by facilitating reactor operation and maintenance and, on the other, by design measures to reduce the immediate and delayed consequences of accidents to members of the public (in particular the population in the vicinity of the plant) and to operating staff. Research and development activities carried out in support of the EPR design, notably on severe accidents, have contributed to the knowledge of accident phenomena and helped to enhance the safety level of the plant design.

With regard to reducing the potential consequences of incidents and accidents, defence in depth is improved in four main ways:

- By accounting for, and reducing the frequency of initiating events (which cause transients, incidents or accidents) liable to occur during the different states which the reactor may encounter during operation (including full power and shutdown states, and states with the core completely unloaded in the spent fuel pool). Taking internal hazards into account on a deterministic basis in accordance with design principles similar to those used for simple initiating events, enhances the defence in depth approach (see section 1.2.3 in this sub-chapter).

- By taking into account external hazards at high severity levels, whether the hazards are of human origin (aircraft crashes, explosions…) or of natural origin (earthquakes, extreme temperatures…). In addition to their direct effects, these hazards are studied from the point of view of the damage they may cause on non protected structures and equipment, inside or outside the plant (see section 1.2.3 in this sub-chapter).

- By taking severe accidents into account at the design stage, and implementing physical measures to ensure "practical elimination" (see section 1.2.3 in this sub-chapter) of events and sequences that could have a significant radiological impact on the environment during the power plant service life. For events which cannot be prevented by design, the probability of environmental releases is minimised by strengthening the containment, including conditions which could lead to containment bypass.

- By use of Probabilistic Safety Analyses (PSA) at the concept design phase to confirm the design approach and identify the multiple failure sequences that should be considered in the design basis, so as to prevent core meltdown accidents (see section 1.2.6 in this sub-chapter). Within this framework, an overall core meltdown frequency of 10^{-5} per annum per unit is set as a design objective, taking into account all types of failures and hazards (see Sub-chapter 15.0).

In addition to enhancing the defence in depth approach, significant efforts have been made in the reactor design to:

- reduce production of effluents and waste from reactor operation and those arising from dismantling at the end of reactor life,

- improve reactor operation by enabling some maintenance activities to be carried out at power and by reducing operator doses collectively and individually by provisions defined at the design stage,

- consider, in addition to nuclear hazards, all the non-nuclear risks to the environment produced by the plant.

The defence in depth approach to safety, and the significant improvements that have been made to EPR reactor design as a Generation 3+ PWR, are set out and developed in this chapter.

1.2. THE EPR SAFETY AND DESIGN APPROACH

In order to fully understand the issues dealt with in this report, the main design stages of the French EPR programme need to be reviewed and understood.

As an "evolutionary" project based on the latest reactors in operational service in France and Germany, the EPR programme underwent a harmonisation process covering the French and German safety approaches which led to:

- publication at Safety Authorities level in July 1993 of a "joint declaration of French and German Safety Authorities on a common safety approach for future pressurised water reactors” [Ref-1],
- publication in August 1993 of a Conceptual Safety Features Review File (CSFRF) which set out the main safety options proposed for the EPR project [Ref-2].

The requirements and approaches proposed in these two documents served as a basis for the "Basic Design Phase" of the project which was concluded with the submission of a synthesis report (Basic Design Report) to the French and German Safety Authorities in October 1997 [Ref-3].

To enhance the competitiveness of the design, the EPR designers then initiated an additional design study in the "Basic Design Optimisation Phase" (BDOP) during which important design parameters were upgraded and optimised. The reactor power output, the installation of equipment inside the main nuclear island buildings, and the safety system design were reconsidered in the BDOP, which concluded with the submission of an updated version of the Basic Design Report to the French and German Safety Authorities in February 1999 [Ref-4].

The designers then undertook a final study in the "Post BDOP" phase, which involved in-depth studies of the EPR and the submission of additional information to the Safety Authority to support the technical approaches set out in the Basic Design Report. This study led to a series of formal undertakings by the designer on the technical approaches to be followed. These undertakings, together with recommendations of the French safety advisory committee and associated German experts developed in sessions held in the period 19-26 October 2000 and presented in the Technical Guidelines (see Sub-chapter 3.1 - Table 1), formed the framework for the EPR design.

Since then:

- detailed design has been performed,
- on 28 September 2004, the French Safety Authority published a letter on safety options for the EPR reactor project [Ref-5]. This letter confirmed that the Technical Guidelines should have the status of safety requirements.
- EDF decided to construct the first French EPR at Flamanville.

This PCSR for the UK EPR is made up of twenty-one chapters listed in Sub-chapter 1.1. Some of these chapters or sections include the "zero" reference in their numbering, indicating that they contain relevant safety requirements.

The main reactor parameters used for the UK EPR and a detailed comparison of the different design and operating parameters of the EPR reactor and latest-generation reactors (French - N4 and German - Konvoi reactors) are given in Sub-chapter 1.3 of the PCSR.

1.2.1. The defence in depth approach and the different containment barriers

1.2.1.1. Implementation of defence in depth

The safety design of the EPR follows the well established defence in depth approach as presented in IAEA Safety Standard on nuclear reactor design NS-R-1. As noted in section 1.1.2 above, the “defence in depth” concept comprises five levels:

1. A combination of conservative design, quality assurance, and surveillance activities is applied to prevent departures from normal operation.

2. Detection of deviations from normal operation is implemented and protection devices and control systems provided to cope with them (This level of protection is provided to ensure the integrity of the fuel cladding and of the Reactor Coolant Pressure Boundary (RCPB) in order to prevent accidents.)

3. Engineered safety features and protective systems that are provided to mitigate accidents and consequently to prevent their development into severe accidents.

4. Measures are implemented to preserve the integrity of the containment and enable control of severe accidents.

5. Off-site emergency response.

1.2.1.2. Basic objectives, safety functions and barriers

The EPR reactor design has been developed from the design of reactors in current operation. To implement the "defence in depth" principle, successive measures are implemented to achieve the three main safety functions that are:

- Control of fuel reactivity,

- Fuel heat removal and,

- Containment of radioactive material.

These include the placing of successive physical barriers between radioactive materials and the environment. In particular, three barriers are used:

- 1st barrier: the fuel cladding,

- 2nd barrier: the reactor coolant pressure boundary,

- 3rd barrier: the containment building.

The EPR design applies operational experience and, for each of the three main safety functions, provides enhanced prevention and/or mitigation of operational incidents and accidents, to give improved protection to the public and operational staff.

The main improvements, for the three main safety functions, are set out below.

Control of fuel reactivity:

- Continued use of the passive system of gravity insertion of rod cluster control assemblies (RCCAs), installation of a heavy reflector between the fuel and the core barrel to enhance neutron reflection, increase of core margins by use of a lower linear power density in the fuel and use of fixed, in-core instrumentation to ensure permanent monitoring of specified core parameters.

  This design aspect is dealt with in Chapter 4.

- Separation of safety and operational functions within the boration system, through the creation of a system dedicated to emergency boration consisting of two redundant trains, each fitted with a pump and borated water storage tank located in the fuel building. Each train is individually able to bring the reactor back to a safe state after an accident. This system is separate from the safety injection system.

  This design aspect is dealt with in Sub-chapter 6.7.

- A systematic search for various conditions which might lead to boron dilution of the primary coolant and inclusion of monitoring systems to stop inadvertent dilution in most situations and to preclude its occurrence in others by suitable design improvements,

  This design aspect is dealt with in Chapters 14 and 16.

Fuel heat removal:

- Creation of a system combining the functions of safety injection and shutdown cooling of the reactor, organised into four separate, independent trains. Each train is fitted with an accumulator located inside the reactor building, injecting emergency cooling water into the primary cooling system cold legs. Outside the reactor building, each train comprises a low-pressure injection pump, a medium-pressure injection pump and a heat exchanger. In injection mode, system alignment enables water from the RIS [SIS] tank (In-Containment Refuelling Water Storage Tank (IRWST) located in the reactor building) to be injected into the reactor coolant system (RCP [RCS]) cold legs. Alternatively, the system can be switched to cooling mode, enabling the low-pressure pumps to be supplied from the hot legs and to re-inject water into the cold legs via the heat exchanger.

  This design aspect is dealt with in Sub-chapter 6.3.

- Total separation of the steam generator auxiliary feedwater supply function from the feedwater supply used in reactor start-up and shutdown, the latter being provided by a dedicated system. The auxiliary feedwater system comprises four trains, each with its own water tank and pump, which supplying separately one of the four steam generators. Two headers connecting the four trains make it possible to provide mutual emergency back-up in the event of the failure of one of the four pumps. Because the SG auxiliary feedwater system comprises four trains, it offers enhanced resistance to common cause failures, in particular those resulting from external hazards.

  This design aspect is dealt with in Sub-chapter 6.6.

- Installation of a heat removal system outside the containment for use in severe accident conditions. This is a two-train system, each train containing a pump and a heat exchanger, which is capable of cooling the containment by spraying, and also of cooling the corium in the corium spreading chamber. Both trains are required to begin operation within 12 hours, and to continue operating for at least two weeks following the accident. Residual heat removal can be performed by a single train after two weeks.

  This design aspect is dealt with in Sub-chapter 6.2.

- Installation of a borated water tank inside the reactor building to supply reactor emergency cooling systems and the primary coolant chemical and volume control system as well the containment heat removal system used in the event of a severe accident. Having this tank avoids the need to switch to recirculation mode in post accident conditions and also offers enhanced protection to the water supply following external hazards.

  This design aspect is dealt with in Chapter 6.

- Improved design of the cooling system using the essential service-water and component cooling systems so as to significantly reduce the frequency of total loss of heat sink as an initiating event. The design comprises a main system arranged in four separate and independent trains each fitted with a pump and a heat exchanger. In addition, the main system is backed up by a dedicated circuit comprising two trains fed by specific power supplies which enable heat from corium cooling to be removed in severe accident conditions in the event of a total loss of heat sink.

  This design aspect is dealt with in Sub-chapter 9.2.

- Finally, for conditions where fuel is partly or totally located in the fuel building, a reduction in the sensitivity to the unavailability of equipment. This is achieved by the installation of two pumps on the two main loops of the cooling system. Moreover, the risk of fuel element melting in the pool is ‘practically eliminated’ by the inclusion of a third cooling system that mitigates the effects of the loss of the two main cooling trains. Provisions are also implemented to prevent and/or mitigate the effect of accidental draining of the spent fuel pool.

  This design aspect is dealt with in Sub-chapters 9.1 and 16.3.

<u>Containment of radioactive material</u>:

- Provisions are implemented on the EPR to contain radioactive material, mainly in respect of the reactor and connected buildings. These provisions are set out in Sub-chapter 3.3 which deals with design of the third barrier (i.e. the containment building).

1.2.1.3. Design of the fuel (first barrier)

The EPR reactor core includes 241 17 x 17 assemblies, each comprising 24 guide tubes and 265 fuel rods. This design uses a relatively low average linear power density and helps to preserve significant core margins (during normal operation and accidents) while at the same time enabling implementation of the most efficient low neutron leakage loading patterns. The maximum targeted burnup fraction is consistent with what is scheduled to be implemented over the medium-term throughout the French reactor network. This fuel is not fundamentally different in terms of technology from that currently used in the French and German reactors.

An important objective of the core design is to reduce the incidence of clad cracking via pellet-cladding interaction or stress corrosion, and a design not prone to this phenomenon will be used. Use of a specifically selected cladding alloy, together with the installation of new instrumentation (based on sensors uniformly distributed throughout the core), contribute towards attaining this objective.

A qualification programme on fuel pellets, cladding material and assembly structure is currently being carried out. This programme will make it possible over the coming years to refine the design of EPR fuel.

The possibility for different kinds of fuel management has been deliberately left wide for optimum flexibility of future EPR operation. Benchmark forms of management envisaged are based on a UO2 core with a cycle of 12, 18 or 22 months and on a 30% MOX core with an 18-month cycle. In addition, its large core makes the EPR well suited for use of more advanced fuels, thereby optimising long-term plutonium stock management (single- and multi-recycling of Pu).

This design aspect is dealt with in Chapter 4.

1.2.1.4. Design of pressurised envelope (second barrier)

1.2.1.4.1. Reactor Coolant System design

In line with the defence in depth approach, the primary cooling system design achieves the double requirement of reducing the frequency of initiating events (by having larger operating margins and increased system inertia) and reducing the consequences of initiating events if they occur. Sub-chapter 3.1 - Figure 1 with the associated comments here below identify improvements made to the primary cooling system relative to previous generation reactors.

For prevention of primary component failures for which protection cannot be practicably provided, and for which the consequences of failure would be unacceptable or where the acceptability of failure in general has not been fully justified, a set of specific measures are taken into consideration to achieve and demonstrate the high integrity of those components. These components, designated High Integrity Components (HIC), are listed below and detailed in Sub-chapter 3.4. The specific measures taken for individual HIC components are discussed in the sections of the PCSR dedicated to those components.

- Reactor Pressure Vessel ①: to accommodate a large core of 241 assemblies, the vessel has an increased diameter and is fitted with a heavy reflector located between the fuel and the core barrel. The reflector is made up of a stack of twelve forged plates, which are attached to the lower core plate by a set of keys and anchor rods. This design avoids the use of welded or bolted assemblies in the vicinity of the core. The reflector reduces neutron leakage and shields the vessel, thus limiting its lifetime neutron dose. The nozzle support ring and the vessel flange are made from a single forging formed from a large single ingot; this eliminates the very thick circular welding which exists between these two components in the pressure vessels currently used in the EDF fleet. Moreover, the design of reactor internals has benefited from a detailed simulation of thermo-hydraulic phenomena in normal operating conditions and most accident conditions.
    - o The Reactor Pressure Vessel is a HIC.

- Vessel head ②: the design of the vessel head and control rod drive mechanisms is based on that used in German units, enabling core instrumentation to be installed from the top, and removing the need for associated penetrations in the vessel bottom head. The core instrumentation uses an “aeroball” system which comprises twelve nozzles for neutron and thermal instrumentation around the head. This solution is made possible by the low overall dimensions of the control rod drive mechanisms (RGL [CRDM]) which, in addition, do not need a forced ventilation cooling system. In all, the head is fitted with 106 penetrations (89 for the RGL [CRDM], 16 for the instrumentation and 1 for a vent line).
    - The Vessel Head is a HIC.
- Primary coolant pump ③: the primary coolant pumps benefit from French design feedback and include design improvements to reduce the risk of erosion by cavitation, which has been experienced on the N4 design. In addition, these modifications result in improved performance. Also, in addition to the multiple successive seals at the pump shaft penetration, the pumps are fitted with a shutdown sealing device designed to reduce the risks of reactor coolant leakage in conditions which might cause damage to the main standstill seals (i.e. total loss of power supply or cooling water).
    - The reactor coolant pump bowl casings (and flywheel) are HIC.
- Steam Generators ④: by increasing the internal volume of the SGs (in comparison to the previous generation of reactors), the effects of transients are reduced. Other improvements over the N4 design SGs that increase the heat exchanger efficiency are: increase of the heat exchange area and the saturation pressure, and improvements in fluid flow at the spacer plate level. In addition, the choice of material for the SG tubes has benefited from feedback from operating French plants.
    - The steam generators (pressure boundary parts) are HIC
- Pressuriser ⑤: as with the SGs, increased internal pressuriser volume helps to mitigate transients. Additionally, maintaining a two-phase condition when shutting down (by gradual injection of nitrogen during depressurisation) reduces the risk of overpressure inherent in single-phase operation. Finally, changes to the spray system design reduce both nozzle loading and fatigue risk on the forged shell.
    - The pressuriser (pressure boundary parts) is a HIC.
- For pressure protection of the RCP [RCS], the upper section of the pressuriser is fitted with 5 relief lines which are connected to a common relief line discharging towards the Pressure Relief Tank. The first three relief lines (connected to the pressuriser by three dedicated nozzles) ⑥ enable the primary coolant to be discharged to a relief tank via automatic pilot-operated pressure relief valves. The two other relief lines (connected to the pressuriser by a single nozzle) ⑦ are dedicated to mitigation of severe accident conditions and allow depressurisation of the RCP [RCS] to prevent overpressure.

- The main reactor coolant loop pipework ⑧ : due to improvement of the forging process, the number of welds has been significantly reduced (9 welds per loop compared to 12 on the N4 design). This has been achieved by machining large nozzles and one bend directly in the legs instead of welding. The welding of homogeneous welds was also significantly improved using a high quality automated welding process which enables a significant reduction of the volume of weld metal, and as a consequence considerably improves the inspectability of the welds. Moreover, this reduction in the number of welds contributes to a reduction of the risks of fatigue and local hydraulic phenomena. The Main Coolant Lines are HIC so that a double-ended guillotine break of the Main Coolant Lines is discounted as a design basis event and the RCP [RCS] design basis accident becomes a break of the largest connected pipe, i.e. the pressuriser surge line which links the pressuriser ⑤ to the hot leg.

  Although the MCL are designated as HIC for the UK EPR and the associated requirements are described in Sub-chapter 3.4, the “Break Preclusion Concept” remains in the current version of the PCSR to explain why the 2A-LOCA is not considered in the design basis, and why the Surge Line break is the largest large break LOCA considered as PCC-4 event. In fact, the HIC claim includes requirements which make up three legs of the break preclusion concept (prevention, surveillance and mitigation). An additional leg of the break preclusion concept (risk reduction) is not considered part of the HIC claim, but as an additional conservative measure.

- Adjustment of the relative elevations of the different components, i.e. the vessel, the primary coolant loops and the steam generators has made it possible to reduce the requirement for operating at mid-loop during shutdown phases and also gives reduced sensitivity to uncovering the core in Loss Of Coolant Accident (LOCA) conditions.

  Design of the RCP [RCS] and its components is dealt with in Chapter 5.

1.2.1.4.2. Secondary Cooling System design

The design of the secondary cooling system also involves improvements which mainly affect the steam system, namely:

- The demonstration of the acceptability of failure of the Main Steam Lines (MSL) has not been performed exhaustively, therefore the main secondary pipework ⑩ (MSL inside containment and outside containment up to the Terminal Fixed Point (TFP) downstream of the Main Steam Isolation Valve (MSIV)) is designated HIC, including the pressure boundary parts of the MSIV. As a result, the guillotine break of this pipework or valve is not considered in the design basis as an initiating event. This HIC claim is not applied to SG feedwater piping ⑨.

  Despite this HIC designation for the UK EPR and the associated requirements described in Sub-chapter 3.4, the “Break Preclusion Concept” remains in the current version of the PCSR to explain why the double-ended MSL break is not considered in the design basis. In fact, the HIC claim includes requirements which make up three legs of the break preclusion concept (prevention, surveillance and mitigation). An additional leg of the break preclusion concept (risk reduction) is not considered part of the HIC claim, but as an additional conservative measure.

- All the steam relief valves, pressure relief valves and main steam isolation valves form a more compact steam system ⑪, the mechanical design of which eliminates the risk of consequential damage.

Design of the secondary cooling system is dealt with in Chapter 10.

1.2.1.5. Design of civil engineering structures (third barrier)

In the EPR reactor design, the civil structures fulfil a dual function:

- protecting the plant from all hazards addressed within the reactor design basis, both internal and external,
- protecting the environment in accident conditions that have not been "practically eliminated" and in particular limiting the need for protective measures in the most severe conditions (RRC-B).

With regard to internal events, the structural design must take into account a low-pressure core meltdown with margins to allow for uncertainties in the current knowledge of such phenomena,

With regard to external events, the structural design is required to take into account the most severe loadings, whether these are due to natural phenomena such as earthquakes or extreme weather conditions, or to human activities such as explosions and aircraft crashes.

Within this framework, a dedicated sub-chapter of this PCSR is provided, aimed at:

- listing the different standard and site-specific structures (including metallic structures) within the EPR nuclear island,
- setting out the detailed safety requirements to be considered during the design,
- introducing the design code used (ETC-C) and summarising the main corresponding civil engineering criteria.

The requirements and design bases chosen for civil engineering structures are set out in Sub-chapter 3.3.

<u>The third containment</u> barrier constitutes the final protection against radiological consequences arising from accident conditions in the event of failure of the first two barriers, in particular following core meltdown. In such conditions, protection of the public living in the vicinity of the plant and compliance with corresponding radiological requirements are based on a set of constructional provisions applied to buildings, equipment and systems, referred to as the containment function.

These constructional provisions are aimed at ensuring that radioactive products are retained inside the buildings in question. These include the reactor building itself and any connected buildings which are liable to be contaminated. Containment integrity requirements are thus defined for all buildings involved in different postulated accident conditions.

The main provisions for containment of radioactive materials and for the protection of this containment are shown schematically in Sub-chapter 3.1 - Figure 2.

1.2.1.5.1. Containment description

With regard to the reactor building, the design chosen is based on the concept of a concrete double-walled containment similar to that used for the latest-generation reactors in the French network. These have been upgraded to enhance defence in depth, mainly by addressing phenomena linked to low-pressure core meltdown. Individual design improvements are described below. The numbering refers to Sub-chapter 3.1 – Figure 2:

- A metal liner is included, covering the whole internal face of the inner containment ① so as to guarantee very low leakage; the space ② between the inner and outer containment walls is maintained at negative pressure, enabling collection of any leakage from the inner containment and filtration before release to the atmosphere.

- All leakage paths liable to place the inside of the containment in direct contact with the external environment are eliminated. All containment penetrations ③ emerge into connecting buildings so that leakages may be collected and filtered.

- Additional water capacity is installed in the containment, in particular to improve control of both design basis and severe accidents. Having this additional capacity (the In-containment Refuelling Water Storage Tank (IRWST) ⑥) makes it possible to supply dedicated systems situated in the safeguard building rooms ⑦ via direct suction from the separate sumps ⑧ thereby limiting the possibility of failure linked to switchover during recirculation.

- A system is designed to recover and spread corium ⑨ resulting from core meltdown and low-pressure release from the vessel. In terms of civil engineering, this system consists of a channel which directs the gravitational flow of corium into a large spreading chamber whose floor is covered with a layer of sacrificial material that protects the foundation raft. The thickness of the raft has been increased, thereby preventing penetration by corium. The arrival of the melt in the core catcher triggers the opening devices that initiate the gravity driven flow of water from the IRWST into the spreading compartment.

- The inner containment (and its pre-stressing) design take into account the effects of pressure (and temperature) of the different core meltdown scenarios considered. In particular, effects due to explosion of the maximum quantity of hydrogen produced during such conditions are included.

- An active system is implemented for ultimate cooling of the containment based on containment sprays and removal of residual heat from the corium using the IRWST water. This system comprises two identical cooling trains designed to remove residual heat from the containment without the need for venting. Operation of both trains is required during the first two weeks following the accident, with a single train having adequate capacity thereafter.

- Additional margins are introduced into the containment design by defining two "grace periods". The first period applies to the inner containment and is aimed at ensuring containment leak-tightness for a twelve-hour period after the beginning of the core meltdown scenario, without the need for operation of the ultimate containment cooling system referred to in the previous paragraph. The second grace period applies to the inter-containment space. The inner and outer containment buildings are designed so as to ensure a grace period during which the inter-containment space will remain at a negative pressure even if the inter-space ventilation fails when the accident occurs.

- Finally, in order to enhance radiation protection for staff during permitted access in the reactor building for maintenance activities during operation, two zones have been created inside the containment area. The first zone (Z1) includes the entire RCP [RCS] and is considered as being inaccessible during power operation. It is isolated from the rest of the containment (Z2 zone) by extremely thick concrete shells or by metal protective devices. In the event of an accident, these devices withdraw so as to make all the free space in the containment available for gaseous expansion, in order to prevent build-up of hazardous gaseous concentrations.

The containment design is set out in Sub-chapter 6.2.

1.2.1.5.2. Inner containment design

The metal liner anchored to the inner containment internal wall makes it possible, for the containment function to combine leak-tightness capability with the mechanical ability to withstand internal pressure. With this approach, the metal liner provides leak-tightness, and the pressure capability is ensured by the pre-stressed concrete inner containment walls. The design is similar to that implemented in French 900 MW plant.

Building on the experience gained in designing such containments, the EPR design is based on the concept of a design pressure, a maximum test pressure and a leak tightness pressure.

The design pressure is the basis for the design of the entire civil structure, and specifically the pre-stressed concrete. It envelopes all pressures occurring under all design basis transients, incidents or accidents (Plant Condition Categories PCC-2 to PCC-4) or multiple failures or core melt accidents (Risk Reduction Categories RRC-A and B). On the basis of relevant studies, a design pressure of 0.55 MPa absolute has been adopted for the EPR inner containment.

To demonstrate that the design and construction of the internal containment are satisfactory in terms of both leak tightness and pressure capability, an initial test is performed at ambient temperature. In the test, the pressure is progressively increased, with a series of pressure hold-points and associated measurements. The containment leakage rate is measured at design pressure, i.e. 0.55 MPa absolute. The test is then extended to a pressure of 0.6 MPa, which is termed the maximum test pressure. This increased test pressure takes account of the effects of temperature on the steel liner and thrust exerted by the liner on the concrete structure at the maximum temperature achieved under accident conditions (170°C). The stress measured at this pressure serves as justification of the pressure capability of the inner containment1.

To reinforce the defence in depth aspects of the design, the verification programme is extended beyond the design pressure and maximum test pressure, to the leak tightness pressure for the inner containment. This confirms the existence of margins in the design. It enables the leak tightness of the containment to be confirmed in extreme core meltdown accident conditions for which phenomena exacerbating the risk have been taken into account. The leak tightness pressure is set at 0.65 MPa absolute.

Sub-chapter 3.1 – Figure 5 shows the different pressure values considered in the design of the EPR inner containment.

1.2.1.5.3. Buildings contributing to the containment function and the avoidance of containment bypass

Since the EPR installation is designed in such a way that all penetrations emerge into connecting buildings, these buildings play an important role in containing radioactive products. The connecting buildings concerned are the four divisions of the safeguard building, the fuel buildings and, to a lesser extent, the nuclear auxiliary building (schematic diagram shown in Sub-chapter 3.1 – Figure 2). The design objective is that filtering of any possible radioactive leakages into these buildings must be ensured.

[1] It should be noted that the pressure values indicated here only concern pre-operational containment acceptance tests. They do not give any advance indication of the pressure values to be chosen for periodic containment tests.

Identifying and eliminating potential routes for containment bypass has utilised feedback from studies of the existing EDF fleet, taking account of features specific to the EPR. As part of the in-depth studies, three groups of potential bypass conditions have been defined and analysed (see Sub-chapter 16.3), namely:

- bypasses caused by initiating events on systems connected to the primary cooling system due in particular to failure of isolating valves. The main systems concerned are the RIS/RRA [SIS/RHRS], the Chemical and Volume Control System (RCV [CVCS]) and the primary sampling system,

- bypasses caused by accident sequences such as an Steam Generator Tube Rupture (SGTR) aggravated by a stuck open safety valve ,

- bypasses resulting from severe accidents or core meltdown sequences such as single or multiple SGTRs caused by a severe accident.

Some of these bypasses are excluded by specific design provisions. Others are controlled in such a way as to prevent them leading to a core meltdown situation (e.g. failure of the RIS/RRA [SIS/RHRS] system in residual heat removal mode).

In order to validate the adequacy of EPR design against containment bypass events, functional analysis and quantification of the potential initiators were performed. These studies evaluate the risk of bypass for each of the scenarios considered using PSA methods and show that the risk of bypass is very low.

This design aspect is set out in Chapters 6 and 15, and Sub-chapter 16.3.

1.2.1.5.4. Containment during shutdown states and spent fuel management

The containment study also covers conditions in which the RCP [RCS] is open and the core is unloaded and stored in the fuel building pool. In these conditions, equipment access hatch reclosing times have been defined on the basis of transient analysis.

For conditions where the core is totally unloaded and cooled in the fuel building pool, a dedicated cooling system has been designed to achieve "practical elimination" of core meltdown.

Risks of rapid draining of the pool are also taken into consideration. Constructional provisions have been included to ensure "practical elimination" of core meltdown in the fuel building following such occurrences.

In addition, the design of systems used during reactor shutdowns, and in particular during fuel handling operations, benefits from all the experience encountered during the operation of the previous French PWRs. For example, the fuel-handling machine is fitted with a device which prevents fuel element positioning errors during reloading operations.

This design aspect is set out in Chapters 9 and 15.

1.2.1.5.5. Design of structures shared by the nuclear island

The raft foundation and the shell which gives protection from aircraft crashes are two structures which are shared by all, or a large part of the nuclear island. They are constructed on the following principles:

- The foundation raft is cross-shaped with a side length of approximately 100 metres. It is the shared base for the reactor building, the fuel building and the four safeguard building divisions. Its extremely thick foundation ensures the relative stability of the buildings it bears. Within the reactor building, the foundation raft houses the corium recovery and cooling plant,

- The aircraft shell is designed to protect the reactor building, the fuel building and Divisions 2 and 3 of the safeguard building against military and commercial aircraft crashes. It comprises an extremely thick concrete shell covering the roofing and surrounding the exterior walls of the fuel building and Divisions 2 and 3 of the safeguard building.

  This design aspect is set out in Sub-chapter 3.3.

1.2.2. Integrating operation and maintenance into the design: architectural effects

1.2.2.1. Preventive maintenance

A design based on four safety trains means that maintenance is possible on one train when the reactor is at power. Note that this preventive maintenance is taken into account in EPR accident studies. Application of the two-zone concept to the reactor building, mentioned above, enables preparation and completion of planned maintenance operations in this building to take place over a period of ten days around a refuelling outage. The "two zone" concept is described more fully in the section relating to the ETY (Combustible Gas Combustion Control) system in Sub-chapter 6.2.

Maintenance operations that are scheduled around shutdowns have been subjected to a review aimed at improving conditions for staff. As an illustration, the opening diameters for access to the EPR steam generator secondary and primary sides have been increased in comparison with previous SGs designs to facilitate access for staff and inspection equipment.

This design aspect is set out in Sub-chapter 18.2.

1.2.2.2. Radiation protection

The objective of reducing occupational exposure of workers has been implemented by carrying out an optimisation process at the EPR design stage based on feedback from the French PWR fleet. In this respect, the As Low As Reasonably Achievable (ALARA) approach has been implemented by taking account of feedback from the best plants in the French fleet. This makes it possible to define an ambitious collective dose objective.

For the EPR, the objective for the collective dose for plant staff is set at 0.35 man.Sievert per reactor year (to date, the average collective dose incurred in Nuclear Power Plants (NPPs) of the OECD countries is about 1 man.Sievert per reactor year; therefore the EPR target represents a significant reduction).

A first estimate of the assessed collective dose has been performed considering the current state of the design: this will be fine-tuned to ensure that the collective dose objective has been achieved. Reduction of individual doses is achieved by focusing optimisation actions on those activities with a relatively high dose burden. This assessment requires identification of radioactive sources as well as design enhancements. As an illustration:

- the design of the vessel head is such that replacing Control Rod Drive Mechanisms RGL [CRDMs] (a bolted connection between the casing flange and the adapter flange) enables a 40-fold reduction of the dose received by staff during such operations.

- placing a concrete floor at the top of the pressuriser at safety valve level, together with a new heater arrangement (allowing automatic dismantling) makes it possible to reduce the associated dose 5-fold for the corresponding maintenance operations.

This design aspect is set out in Chapter 12.

1.2.2.3. Instrumentation and Control

Digital technology is used for both safety-related and operational instrumentation and control (I&C) in order to take maximum benefit from the experience gained on modern operating plants. Use of this proven technology gives advantages in terms of the man-machine interface and implementation of diversity.

The physical structure of I&C systems and equipment is designed to provide adequate independence between functions which are required within the different levels of defence in depth.

Provisions such as hardware and software diversity must be implemented to preclude software-induced common cause failures.

These design aspects are dealt with in Chapter 7 of the PCSR.

1.2.2.4. Human Factors

Due consideration has been given to Human Factors (HF) throughout the design process, taking into account operation, testing and maintenance. The overall objective is to ensure that the risk of human failure events (which encompasses both human errors and violations) adversely affecting nuclear safety is ALARP for the generic design of the UK EPR. The application of Human Factors approaches contributes to ALARP objectives through the following:

- Human Factors studies of predecessor design and operating concepts to identify strengths to be retained, and evaluate options for improvements;

- the identification and analysis of Human Based Safety Claims (HBSC) and the identification/substantiation of controls to mitigate risks;

- more broadly through the integration of Human Factors principles, standards requirements and assessments to the design of the UK EPR.

Human Factors also contributes to achieving the radiation protection objectives (discussed in Sub-chapter 12.0).

The HF element of the UK EPR safety case is presented in Sub-chapter 18.1, and is based on the results of:

- the Human Factors Engineering (HFE) programme for the EPR Flamanville 3 (FA3) Initial Reference Design;
- additional HF analyses and reviews to meet UK requirements and context.

The HFE programme for the FA3 Initial Reference Design covers both the nuclear and conventional islands, including the Main Control Room (MCR), Remote Shutdown Station (RSS) and other plant locations where operations and maintenance activities take place. The HFE programme includes all plant operating categories, including normal, emergency and Severe Accident management operation. Particular emphasis has been given to the MCR, as this is the main location for monitoring and control of the plant.

Due consideration has also been given to HF issues associated with maintenance and testing, and to other activities with high nuclear safety, security, environmental, and availability requirements, or for which certain technical changes have been envisaged. These include, for example, fuel handling, steam generator inspection, Reactor Coolant Pump maintenance, and waste processing.

Some additional HF activities have been carried out in support of the safety demonstration to address differences between French and UK licensing requirements and safety case practices. Key differences include the principle of demonstration of ALARP, the claims-argument-evidence approach to safety cases, and the expectation to substantiate Human Based Safety Claims in the safety case using recognised HF methods such as task analysis. The scope of UK EPR specific HF activities includes:

- identification and analysis of pre-fault human actions during normal operation that may degrade mitigation system availability (Type A claims), or contribute to an initiating event (Type B claims);
- task analysis and substantiation of risk significant post-fault HBSCs (Type C claims). This includes both MCR and local-to-plant actions.
- analysis of specific HBSCs in the deterministic safety analyses. (Steam Generator Tube Rupture of a single tube, heterogeneous boron dilution, Internal Flooding and Dropped Loads);
- identification of ‘holistic’ claims on aspects of UK EPR design and operation which support human reliability, and development of supporting arguments and evidence to substantiate these;
- identification of inputs to the design of UK EPR specific systems.

Human errors are considered in the design basis analysis via the definition of design basis initiating events and through the rules applied in treating operator actions claimed in response to design basis events (see section 1.2.3.1 below). The design basis analysis explicitly identifies a number of claims on operator actions. Additional implicit claims associated with nuclear risk significant plant and equipment have been identified by Human Factors studies. The substantiation of explicit and implicit design basis claims on human reliability is discussed in Sub-chapter 18.1.

A number of Human Based Safety Claims associated with Severe Accident response (Sub-chapter 16.2) and Internal Hazards (Sub-chapter 13.2) have also been identified during the generic design phase and assessed through task analysis. These are also discussed in Sub-chapter 18.1.

A comprehensive analysis of the risk from human errors is presented in the PSA for the UK EPR given in Chapter 15 of the PCSR. The PSA includes the following types of human errors, which include both errors of omission and errors of commission:

- operator errors that could result in initiating events, such as actions causing a spurious trip of the reactor, accidental mis-setting of set-points causing inadvertent boron dilution, etc. These errors are included through their contribution to the assumed frequency of initiating events.

- errors in carrying out tasks that could affect the course of an accident (e.g. maintenance errors). Such errors include instrument calibration errors, equipment design and manufacturing errors, data entry errors that could affect the reliability of data processing equipment, etc. Such errors are included via the values assumed for equipment unavailabilities and Common Cause Failure (CCF) values.

- errors in carrying out actions required in accident management. These errors are represented through basic event data used in the PSA.

The process and results of the Task Analyses for risk significant Human Based Safety Claims in the PSA are summarised in Sub-chapter 18.1.

Sub-chapters 18.2 and 18.3 present additional descriptions relating to normal and abnormal operation of the UK EPR. Chapter 7 presents the principles for, and descriptions of, the UK EPR I&C. This includes the Human-Machine Interfaces in the MCR and other plant locations.

1.2.3. Design scope

The object of the design scope is to define the events taken into account in the Design Basis and to categorise them. The Probabilistic Safety Analysis is a confirmatory step which is used to close the design loop.

The initiating events considered are of two different types and are dealt with differently:

- Internal Faults (turbine trip, LOCA, total loss of feedwater, Anticipated Transient Without Scram (ATWS), etc).

- Internal and External Hazards (fire, earthquake, etc).

In terms of the design process, the overall approach for these two types of initiating events is the same:

a. Definition of the design basis list of events/sequences with consideration of combinations.

b. Quantification of the event/sequence impacts, the results being used for the design of systems and structures and/or the demonstration that the safety requirements are met.

c. Design Verification: this completes the safety analysis by providing a further demonstration that the safety requirements are met. It invariably includes the use of Probabilistic Safety Analysis, and in some cases a deterministic verification is carried out. This step can result in design feedback.

In the following sections the following is presented:

- Design basis analysis of internal faults: this corresponds to items a and b above
- Risk reduction analysis which is aimed at the avoidance of core meltdown: this corresponds in part to point c above.
- Severe accident analysis which is aimed at the mitigation of core meltdown accidents: this corresponds to the items a and b specifically for core meltdown accidents.
- “Practically eliminated” situations: this focuses on the analysis of the risk of Large Early Releases. It is corresponds in part to item c.
- Hazards Analysis which involves the three legs: Hazard Identification (a), Hazard Protection Design Basis (b) and Design Verification (c).
- The fault and protection schedule established as part of the safety schedule

Probabilistic Safety Analysis (PSA) is discussed in section 1.2.6.

1.2.3.1. Internal faults Design Basis Analysis

The safety approach applied to the EPR requires consideration of a limited number of representative internal faults and enveloping conditions liable to be encountered during operation and various associated reactor states. These initiating events are grouped together in four categories based on their estimated frequency of occurrence and their impact on the environment.

On this basis, events are grouped into four Plant Condition Categories (PCCs) as follows:

- PCC-1 which includes all normal operating conditions, characterised by initiating events whose estimated frequency of occurrence is greater than 1 per year,
- PCC-2 which includes design basis transients, characterised by initiating events with an estimated frequency of occurrence in the range of 10^{-2} to 1 per year,
- PCC-3 which includes all design basis incidents, characterised by initiating events with an estimated frequency of occurrence is within the range of 10^{-4} to 10^{-2} per year,
- PCC-4 which includes all design basis accidents, characterised by initiating events with an frequency of occurrence is within the range of 10^{-6} to 10^{-4} per year.

Identification of these events and their classification by category determines the design of systems intended to control them, preventing unacceptable consequences for the plant or the environment.

The list of events considered for the EPR design basis is drawn up in accordance with the process shown in Sub-chapter 3.1 – Figure 3. This process follows the stages set out below:

- As an "evolutionary" reactor, an initial list of EPR design basis conditions was drawn up prior to the Basic Design phase in accordance with guidelines adopted for the design. Full account was taken of the fault/event schedules considered in the latest French and German PWR designs [Ref-1].

- During the Basic Design (BD), this schedule also underwent changes as a result of in-depth studies and development of the EPR design. Further changes were made to respond to requirements arising from the French Safety Authority's project review. This development included a precise definition of the various reactor states and consideration of events likely to occur in peripheral buildings. Certain events found to be unrepresentative of the developing EPR design were excluded. Ultimately, a schedule of postulated events was produced at the end of the Basic Design process to serve as input for the Detailed Design (DD) studies.

- The above process led, at the end of the Basic Design phase, to a set of events and detailed supporting documentation that has been reviewed by the French Safety Authority (ASN). The internal faults design basis analysis set out in this PCSR is based on this schedule.

Chapter 14 describes the initiating events included in the schedule, the assumptions made in associated studies, and the analysis performed for each event. For accident management, provisions are required to initially control the accident, and subsequently to ensure safe and stable long term conditions. The following principles are applied:

- for any reference initiating event requiring operator action within 30 minutes, an adequate level of automatic protection is provided to render the operator action unnecessary,

- local operator actions on the plant must not be necessary earlier than 1 hour after the operator receives the first significant indication of the occurrence of the event,

- the design must provide sufficient plant autonomy before offsite support is needed.

For any event with the potential for radiological release, the Internal Faults design basis analysis is supplemented by a calculation of its radiological consequences, to confirm that it meets the appropriate criteria.

1.2.3.2. Risk reduction analysis – Prevention of core meltdown

The first Risk Reduction Category is Risk Reduction Category A (RRC-A). The RRC-A category is introduced to complement the deterministic Design Basis Analysis (PCC categories) by considering a set of Design Extension Conditions (DEC) involving multiple failure events. Analysis of DEC is performed using both deterministic and probabilistic considerations, especially through the PSA. Analysis of the DECs is used to identify additional safety measures (so called 'RRC-A features'), which make it possible to prevent the occurrence of severe accidents in these complex situations. An RRC-A feature is a specific system, device or function used to mitigate event sequences not addressed in the Design Basis Analysis of internal faults.

This design aspect is set out in Sub-chapter 16.1.

1.2.3.3. Severe accident analysis – reduction in risk of core meltdown accidents

Severe Accident Analysis is considered as the second Risk Reduction step, (Risk Reduction Category B (RRC-B)). It is mainly based on the analysis of four postulated low-pressure core meltdown sequences. These representative sequences are used to define severe accident mitigation measures, including the systems used to stabilise the molten corium inside the containment, and the system providing containment cooling without the requirement for venting.

RRC-B analysis also helps to:

- define the instrumentation required by the operator and the emergency response team to manage this type of condition,
- specify the qualification requirement of equipment necessary to achieve the safety objectives.

This design aspect is set out in Sub-chapter 16.2.

1.2.3.4. "Practically eliminated" situations

In the EPR context, “Practical Elimination” refers to the implementation of specific design measures to reduce the risk of a large early release of radioactive material to the environment to an insignificant level. To achieve practical elimination, each type of accident sequence that could lead to a large early release of radioactivity is examined and addressed by design measures. Demonstration of practical elimination of an accident sequence may involve deterministic and/or probabilistic considerations, and must take into account uncertainties due to the limited knowledge of physical phenomena involved in severe accident analysis.

Conditions covered by specific treatment leading to their practical elimination are those which are liable to give rise to significant early releases (mainly high-pressure core meltdown sequences). The following sequences are considered particularly in this approach:

- Sequences involving high-pressure core meltdown and direct containment heating,
- Prompt criticality accidents,
- Steam explosion phenomena inside and outside the vessel,
- Hydrogen explosions,
- Containment bypass,
- Fuel meltdown in the spent fuel pool.

This design aspect is set out in Sub-chapter 16.3.

1.2.3.5. Hazards analysis

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.

External and internal hazards that could affect the plant must be identified, and provision made to ensure that the risk from hazards is commensurate with the overall frequency and release targets.

As mentioned in section 1.2.3 above, the overall approach to internal and external hazards is similar to that applied for internal faults, i.e.

- Hazard identification, with consideration of credible combinations and setting up the safety requirements,

- Hazard impact quantification (e.g. specific loads and environmental conditions), and design basis protection of structures, systems and components against the impact,

- Design verification against hazards to confirm that the safety requirements have been fulfilled. This is systematically performed on a case-by-case basis (specific to each hazard, which has different characteristics) with the use of deterministic studies, such as building and equipment response, functional impact including consideration of consequential internal faults (for instance, identification of internal faults induced by an initiating internal fire hazard), etc. This process is supported by probabilistic analysis of hazards. This design verification can lead to design feedback.

Basically the hazard design approach is used to determine prevention and protection features to protect the safety systems. The aim is to prevent a hazard from being the cause of the loss of a safety classified function. Moreover a design objective is to prevent hazards from triggering PCC-3 or PCC-4 Nuclear Steam Supply System (NSSS) events. Evidence has to be provided that, in the event of a hazard, the functions required to bring the reactor to a safe shutdown state and to limit radiological releases can be carried out satisfactorily. In practice the protection is achieved by appropriate sizing, redundancy, diversity and segregation, most generally applying Codes and Standards, Regulations and the Technical Guidelines.

In addition to the hazards Probabilistic Safety Analysis, the design verification step involves deterministic analyses, which use generally event-based approaches, for almost all the hazards.

Hazards are postulated to occur during normal operating conditions or, in some cases, during post accident conditions. Combinations of hazards may be considered, with the exception of combinations which cannot reasonably be anticipated.

Where hazards directly affects the operator (e.g. toxic gasses), the consequences are addressed independently of the operating conditions. Concerning hazards causing damage to the equipment, the design approach is to protect every safety function required by the PCC. The PCC have been defined as the bounding cases of internal fault supposed to occur, in each frequency category, on the NSSS process and include, in their definition the requirement of most adverse conditions. This protection is achieved by designing the equipment to withstand the loads associated with the hazard event, or by providing physical separation between redundant elements so that the safety function can be performed despite the occurrence of the hazard.

The hazards identification is presented in the following sections.

The hazard protection requirements, design basis protection and deterministic verification are presented in PCSR Sub-chapters 13.1 and 13.2, with common principles applicable to all internal or external hazards, and principles specific to each hazard.

The probabilistic safety assessment of hazards is presented in PCSR Sub-chapter 15.2.

1.2.3.5.1. Hazard identification for the EPR design

Internal and external hazards considered in the EPR design have been identified through several steps, the main ones being the following:

As an evolutionary design based on the French and German current plants, French and German safety requirements have been used to make an initial list of hazards to be considered for the EPR design. After consideration of experience feedback from both countries, this first list can be seen as an envelope of the two hazards approaches, both for the list itself and for the definition of the load cases associated with each hazard,

For external hazards, an assessment was performed to check their inter-dependency with transients, incidents and accidents, including severe accidents. This work was used to verify and confirm the initial list and to define the safety objectives associated with each type of hazard [Ref-1].

- Because the EPR plant has the potential to be built in several European countries, a comparison with the list of internal and external hazards defined in the E.U.R. (European Utility Requirements – Sub-chapter 2.1) was performed, confirming the list of hazards to be considered. For the particular case of the earthquake and the seismic level to be taken into account in the EPR design, this comparison led to the choice of the EUR spectra as the design spectra for the EPR plant,

- French and international experience feedback of events and hazards which happened during the EPR design studies was also integrated into the definition of hazards to be considered. This affected, in particular, external flooding for costal sites, extreme high ambient temperature (air and water) and the consideration of commercial aircraft crash.

- In addition to this list and on the basis of existing events, possible combinations of hazards, in particular consequences of external hazards have been assessed. A specific methodology was proposed to consider such combinations in the EPR design.

- In addition to this list, hazards which may be generated by malevolent acts were also considered in the EPR design. For this specific group of hazards, relevant information is handled in accordance with national regulations dealing with security and physical protection.

For the specific situation of a definitive UK site, the characteristics of the site will need to be assessed against the generic EPR approach for hazards with the aim in particular of verifying the completeness of the list and the boundary conditions against any potential local characteristics, such as the direct vicinity of a chemical plant or if the plant is located in a very seismic area.

1.2.3.5.2. Internal hazards protection

Internal hazards are events originating within the site boundary but are external to the NSSS which have the potential to cause adverse conditions or damage inside safety classified buildings. Internal hazards taken into account at design stage are as follows:

- <u>fire</u>, by taking into consideration the three protective elements, namely (i) prevention (using low-combustible materials, implementing specific installation rules and assigning potential fire sources to fire sectors and zones), (ii) containment by compartment and cell breakdown, (iii) detection (via rapid identification of the detection point and triggering of the alarm) and (iv) fire-fighting by local operators, by installed fire protection systems and by mobile fire-fighting units,

- flooding, by taking into consideration potential sources such as plant leakage (pumps, valves, tanks etc.), breaks or through wall cracks in piping, tank overflows, failures of certain tanks or spraying by fire-fighting systems,

- breaks in high-energy piping, tanks, pumps and valves which might cause consequential damage and additional faults. Effects considered are pipe-whip, the impact of hot jets and sprays of water or radioactive material. Flooding from these sources is covered as mentioned in the previous paragraph. Fractures of high energy components can also be prevented by taking into account specific measures to achieve and demonstrate their high integrity. These components are designated High Integrity Components (HIC),

- internal missiles generated for example by the ejection of mechanical items under pressure such as control rods, pressuriser heaters, temperature and pressure probes, valve parts and via failure of rotating equipment (e.g. pumps and turbines). Components such as the reactor coolant pump flywheel are “no missile”, as specific measures are taken into account to achieve and demonstrate their high integrity. The reactor coolant pump flywheel is designated a High Integrity Component (HIC),

- internal explosions: the following potential sources of explosion are considered: internal system explosions, explosions inside buildings caused by the release of explosive gases from internal systems, and explosions outside buildings caused by the breach of pressurised containers or release from a system,

- dropped loads generated by failure of handling equipment during lifting and transportation within the plant.

Consideration of these hazards results in installation rules and/or provisions in each of the buildings concerned. A specific analysis will confirm that the plant is resistant to the identified hazards. This study will be carried out for each of the buildings concerned. The rules will be similar to those used for internal faults (taking into account unavailability due to preventive maintenance operations and a single failure).

This design aspect is set out in Sub-chapter 13.2.

1.2.3.5.3. External hazards

External hazards are natural or man-made hazards that originate externally to the plant and that may have the potential of adversely affecting the safety of the plant. A brief description of external hazards considered in the EPR design is set out below.

- Earthquakes are taken into account by considering design seismic motions in the form of a range of spectra. For safety classified systems, structures and components in the buildings of the standard nuclear installation (nuclear island) the EUR spectra set at 0.25g, is used. For other site structures, which include the pumping station, a site specific spectrum is used in the design. The design process is supplemented by safety analysis aimed at ensuring that assessments are in line with requirements (including seismic margin assessment, see Sub-chapter 15.6) and also to check that single or multiple equipment failures in earthquake conditions entail no unacceptable consequences.

- Aircraft crashes. The risks resulting from air traffic are taken into consideration by dividing such traffic into three types of aircraft, namely general aviation, military and commercial. The aim of significant safety enhancement has led to a more general consideration of the risk of aircraft crash (i.e. military and civil aviation) regardless of the probability of the event occurring. Safety is ensured either by physical separation of redundant buildings or by the existence of a physical screen known as the "aircraft shell".

- Risks associated with the industrial environment and communication routes:

    - External explosions. A standard load combination is defined to represent the incident pressure wave generated by the explosion. For the buildings to be protected, multiplication coefficients are applied to the incident wave to take into account possible reflections from surrounding walls. In addition, an analysis is carried out to confirm that design provisions are adequate from a safety viewpoint.

    - Toxic, corrosive or flammable gases. Other consequences of this type of event, related to the specific site, are taken into account, such as fires outside the site.

    - Other site specific hazards. On a site containing multiple plants the possible conventional or nuclear risk associated with other plant needs to be assessed.

- External flooding. The setting of levels is designed to provide suitable margins, taking due account of flood levels reached in the past, and the potential effects of climate change. The approach incorporates operating feedback from events experienced in the EDF fleet to take into account new aggravating factors (swells, rain etc.) in addition to those originally mentioned in safety rules. Rises in groundwater level are considered within the scope of external flooding either as one potential cause of flooding or as an aggravating factor.

- Extreme weather conditions, including temperature, snow, wind, rain, ice, drought or very low heat sink water level etc. Effects of direct loads on the structures and equipment and the potential for hazards (e.g. wind pressure on walls or the production of heavy missiles) are considered. Load combinations are defined for each of the phenomena in question, taking into account general conditions of plant installation such as, for example, location by the sea. The installation design with regard to detailed site specific factors will be checked in subsequent phases.

- Lightning and electromagnetic interference. Rules covering the design and installation of sensitive equipment (mainly electrical) are defined and implemented in such a way as to protect them, for instance via screens for cabling & wiring or meshes for termination design.

Overall, protection from external hazards is ensured by defining the load combinations to be applied to plant, systems and structures which may be affected. For certain external hazards, the "load combination" approach may be supplemented by an event approach.

This design aspect is set out in Sub-chapter 13.1.

1.2.3.5.4. Other hazards taken into account

In addition to hazards listed in sub-sections 1.2.3.5.2 and 1.2.3.5.3 within this sub-chapter, the EPR plant design takes into account other hazards resulting from acts of malicious intent.

With regards to such hazards, the installation is protected via a series of provisions corresponding to the principles of defence in depth aimed at:

- Preventing malicious acts by ensuring that the installation is placed under permanent surveillance. Some of these measures are visible whilst others are covert.

- Physically protecting the plant from different potential threats. Some elements of this protection are intrinsic provisions designed to provide protection against non-malicious external hazards (such as physical separation of redundant systems or "bunkerisation" of parts of the nuclear island). In addition, there are specific provisions aimed at excluding potential assailants from sensitive zones (such as fences around the plant).

- Making provision for and organising measures (similar to an emergency plan) aimed at limiting the consequences of malicious acts if they occur.

Hazards of a malicious nature taken into account in the EPR design are defined by national civil authorities. Such hazards are taken into account by the designer. The design and analysis of counter-measures are examined by and agreed with the civil authorities.

Details of the protection of the plant and local population against acts of malicious intent are dealt with in specific documents outside the Pre-Construction Safety Report, for reasons of confidentiality.

1.2.3.5.5. Multiple hazards

Feedback on external hazards at both the national and international level has underlined the fact that the plant operator may be confronted with multiple hazard situations, as illustrated by the incident at the Blayais power plant on 27 December 1999 [Ref-1].

For the EPR, different potential combinations of hazards are analysed, based on evaluation of operating feedback. The analysis takes into account:

- combination of physical phenomena inherent in the hazard itself,

- combination of the hazard in question with potentially dependent events or internal or external hazards,

- combination of the hazard with independent internal or external initial conditions.

This approach enables a certain number of hazard combinations to be identified and subsequently taken into account in the EPR design.

This design aspect is set out in Chapter 13.

1.2.3.6. Fault and protection schedule

As a conclusion of the design phase, a fault and protection schedule has been established as part of the safety schedule. It provides a list of all postulated faults with potential unacceptable consequences. It includes all initiating faults, with their frequencies and consequences, the safety systems and beneficial safety-related systems involved, and the overall protection claim.

This design aspect is set out in Sub-chapter 14.7.

1.2.4. Radiological consequences

1.2.4.1. Conditions chosen for assessing radiological consequences

The assessment of radiological consequences must demonstrate the ability of the plant to contain radioactive materials, for all design conditions.

With regards to the reactor, the conditions taken into account in the plant design are presented in the PCSR and are as follows:

- Operating conditions with a single NSSS event (PCC-2, 3 and 4), including PCC-2 events triggered by a hazard. The relating conditions are chosen to maximise the demand on the three basic safety functions, reactivity control, decay heat removal and radioactive product containment.
- Operating conditions with events external to the NSSS, including hazards. In this case the demand is placed on the containment function only. Some PCC events are introduced in the design basis analysis for that purpose (e.g. fuel handling accidents in the fuel building or failure of the gaseous waste treatment tanks).
- Operating conditions with multiple failures (RRC-A)
- Hypothetical severe accidents corresponding to RRC-B low-pressure core meltdown sequences.

1.2.4.2. Objectives related to assessing radiological consequences

For the EPR project, requirements concerning the radiological consequences of accidents (including severe accidents) were set at the design stage.

With regard to transient (PCC-2) conditions, the numerical target for the effective dose to an individual off-site is chosen to be equal to the legal limit for normal operation: 0.3 mSv/yr (see section 3.2.2).

With regard to design basis incidents and accidents (PCC-3 and PCC-4), the principle chosen and specified in the Technical Guidelines (see Sub-chapter 3.1 - Table 1) is expressed as follows:

There should be no requirement for protective countermeasures for the public living nearby: i.e., no evacuation, no need for sheltering and no need for distribution of iodine tablets.

In accordance with these objectives, an estimate of the doses received by the population over a short-term period (7 days) and at the site boundary (500 m from the site) is required in practice. The numerical targets needed to comply with the EPR safety objectives may be adapted to site regulations and guidance. For the Generic Design Assessment, the proposed targets are chosen to be in the lower part of the ICRP dose target ranges, that is to say for PCC-3 and PCC-4:

- effective dose < 10 mSv
- equivalent dose to the thyroid < 100 mSv

In the EPR design, no distinction is made between acceptability criteria for the radiological consequences of PCC-3 and PCC-4 accidents.

This design aspect is set out in Sub-chapter 14.6.

With regard to severe accidents, particular attention has been paid to phenomenological understanding and assessment of consequences at the design stage. Requirements of EPR Technical Guideline are aimed at limiting the impact of a severe accident over time and space, including:

- Limited sheltering,
- No need for emergency evacuation outside the immediate vicinity of the plant,
- No permanent relocation,
- No long-term restrictions on the consumption of foodstuffs.

The dose levels to be assumed for these different protective measures are as follows:

- Short-term measures:
    - Requirement for sheltering: 10 mSv (effective dose)
    - Evacuation: 50 mSv (effective dose)
    - Distribution of iodine tablets: 100 mSv (equivalent dose to the thyroid)
- Medium- and long-term measures:
    - Relocation: 10 mSv / month for prolonged exposure (dose rate due to ground contamination) or 1 Sv (effective dose).

Any restrictions concerning consumption of foodstuffs produced in the vicinity of the plant are governed by relevant European marketing regulations applicable in the event of a nuclear accident or other radiological emergency.

This design aspect is set out in Sub-chapter 16.2.

Main methods and assumptions adopted for assessing radiological consequences

Confirmation that radiological objectives have been met is achieved by analysis of the radiological consequences of selected operating conditions. The basic principles and assumptions for assessing these radiological consequences are summarised below:

- The assessment is based on conservative methods and assumptions,

- Calculating the effective dose includes all potential routes for exposure: external exposure to the plume and deposits, internal exposure via inhalation and ingestion of contaminated foodstuffs. The assessment is for a period of 50 years. Results are evaluated:

    - Doses after 7 days. Doses relating to this phase correspond to exposure of a member of the public in the immediate vicinity of the site at the moment of release. Effective doses received via inhalation, external exposure to the plume and deposits on the ground, and doses absorbed by the thyroid by inhalation, are calculated at a distance of 500 m from the site boundary for an adult and a one year old child.

    - Doses after 50 years. Doses after 50 years represent the effects over the lifetime of a person. In addition to the doses received when the radioactive cloud passed over, doses received over the long term take into account the persistence of ground contamination. People living in the vicinity of the plant are subjected to an external exposure to radioactive deposits on the ground as well as to internal exposure by ingestion of contaminated foodstuffs, over a period of 50 years. These doses are assessed at a distance of 2 km from the point of release.

Methods for calculating doses

The main methods and assumptions for calculating doses (atmospheric scattering of fission products released into the environment, dose conversion factors) are described in Sub-chapters 14.6 and 16.2.

1.2.5. Safety functions, safety classification and associated requirements

The safety of the plant is dependent on the performance of its Structures, Systems and Components (SSCs) in normal, hazard and fault conditions. The purpose of the classification approach presented in Sub-chapter 3.2 is to ensure that the SSCs are systematically designed, manufactured, constructed, commissioned and operated so as to fulfil the three main safety functions, defined in section 1.2.1.2, with an appropriate level of quality.

1.2.5.1. Overview of UK EPR classification approach

This classification approach has been adapted from UK and other recognised international guidance and represents a “functional” approach to classification. The steps in the classification approach can be summarised as follows:

1. Identify safety functions and assign categories based on their importance to safety.

2. Identify the Safety Feature Groups (SFGs), System, Safety Features (SFs), and finally components, which fulfil the safety functions, and assign a classification based on the importance of the safety functions they perform.

3. Link the classification to a set of requirements for design, manufacturing, construction, commissioning and operation, which will ensure that the systems and components that perform or contribute to the safety functions are at the required level of quality.

This classification approach is consistent with the HSE Safety Assessment Principles (SAPs) [Ref-1].

1.2.5.2. Safety Functions identification and categorisation

The three main safety functions defined in section 1.2.1.2 are too high-level to allow technical solutions to be developed, so it is necessary to derive more accurately defined functions, which are specific to the plant type or technology. The classification approach has led to the development of two levels of safety functions:

- Plant Level Safety Functions (PLSF). PLSFs are functional capabilities based on the EPR process, which are defined in order to satisfy the main safety functions.
- Lower Level Safety Functions (LLSF) combines the objective of the PLSF with a level of defence in depth to determine the technical means of achieving the functional and performance requirements.

The LLSFs are categorised in three categories based on their significance to safety:

a) Category A – any function that plays a principal role in ensuring nuclear safety.

b) Category B – any function that makes a significant contribution to nuclear safety.

c) Category C – any other safety function.

This design aspect is set out in Sub-chapter 3.2.

1.2.5.3. Identification and Classification of Safety Feature Groups, Systems, Safety Features and Components

The technical means of achieving the functional and performance requirements of an LLSF are studied through the specific terminology and concept defined in Sub-chapter 3.2: Safety Feature Groups (SFGs), Systems, Safety Features (SFs) and Components. A system is defined as the EPR Coding System (ECS), a Safety Feature is a part of a system, and a Safety Feature Group is a concept that groups all the associated Safety Features that are required to ensure a LLSF.

A safety class recognises the importance to safety of the Systems, Safety Features (SFs) and Components contributing to a LLSF through a Safety Feature Group.

In general, the safety class of an SFG should correspond to the safety category (i.e. Category A corresponds to safety Class 1, Category B to Safety Class 2 and Category C to Safety Class 3) of the safety function (LLSF) ensured. As a general principle, a Safety Feature Group will be classified at the same level as the most highly categorised LLSF to which it contributes.

As a general principle, a Safety Feature will be classified at the same level as the most highly classified SFG to which it contributes. Accordingly, the components belonging to a Safety Feature will be classified at the same level as the Safety Feature.

Under the explanations and conditions developed in Sub-chapter 3.2, some support systems will be assigned a safety class at the system level, based on the highest safety class of the SFs/SFGs they are supporting, as an outcome of the classification approach.

This design aspect is set out in Sub-chapter 3.2.

1.2.5.4. Set of requirements

Requirements are essential for designing robust lines of defence consistent with their importance to safety, captured in the safety class. The requirements are assigned at the SFG level and also at the system or component level as follows:

- SFG level – Architecture requirements:
    - Robustness against single failure - redundancy,
    - Physical separation,
    - Robustness against LOOP,
    - Robustness against earthquake,
    - Qualification for accident conditions (see sub-section 1.2.5.4.2 below),
    - Examination, Maintenance, In-Service Inspection and Testing (EMIT).
- Component or system level - design/manufacturing requirements:
    - Robustness against earthquake, against LOOP and qualification for accident conditions, derived from architecture requirements applied at the SFG level,
    - Design codes and other manufacturing requirements,
    - Level of quality assurance.

    This design aspect is set out in Sub-chapter 3.2 and the applicable design codes are presented in Sub-chapter 3.8.

1.2.5.4.1. Robustness against single failure - redundancy through the Single Failure Criterion

When required, the design of a safety feature group important to safety takes into account the single failure criterion. This requirement for redundancy assists in ensuring high reliability of safety classified safety feature groups designed to maintain the plant within its deterministic design basis.

The single failure taken into account is a random failure independent of the initiating event, which necessitates the safety feature group operation. A short term single failure of a component belonging to the safety feature group is considered, for both active components and passive components.

Consequential failures resulting from the postulated single failure are also considered when applying the single failure criterion (when means are not available to detect the occurrence of a failure and restore the function of the affected safety feature group in a short time period).

A single failure is also taken into account in the design of the active safety feature group providing protection against internal hazards.

An active single failure is defined as:

- either the malfunction of a mechanical or electrical component which requires a mechanical movement to accomplish the specified function (e.g. a relay switchover, start-up of a pump, opening or closing of a valve),
- or the malfunction of an I&C component.

NB: the following failures are excluded when the single failure criterion is applied:

a) failure to open of an accumulator check valve (non-return valve),

b) failure to close of a main steam line isolating valve in the event of rupture of one or several steam generator tubes.

A passive single failure is defined as a failure that occurs in a component which does not need to change state to carry out its function. A passive failure can be:

- a leak in a pressurised fluid system; if such a leakage is not detected and isolated, it is assumed to increase until it reaches a flow rate corresponding to full guillotine rupture;
- another mechanical failure disrupting the normal flow rate of a fluid system.

1.2.5.4.2. Qualification for Accident Conditions

The purpose of qualification for accident conditions is to demonstrate that a component would be able to fulfil its safety functions considering all the postulated environmental conditions and loads to which it may be subjected (normal, incident or accident conditions, including severe accident and hazards).

Internationally recognised methods may be used for qualification, based on RCC-E, KTA or IEEE standards.

This design aspect is set out in PCSR Sub-chapter 3.6 for PCC and RRC events and in Chapter 13 for hazards.

1.2.5.4.3. In-service testing

The UK EPR design has fully acknowledged the general principle that the in-service testing of Safety Feature Groups important to safety, which are not continuously in operation in normal plant conditions, should confirm their availability and ensure their reliability consistently with their performance requirements.

This design aspect is set out in PCSR Sub-chapter 3.2 for the definition of the requirements and in PCSR Sub-chapter 18.2 for further details including Examination, Maintenance In-service Inspection as well as In-service testing (EMIT).

1.2.5.5. Classification and requirements applied to structures

NPP structures have a specific safety role: protecting safety classified components, people and the environment from the harmful effect of ionising radiations. NPP structures house and protect components that perform a safety function.

Two safety classes (safety class 1 and safety class 2) and the associated requirements (robustness against earthquake, EMIT, design codes, standards and other manufacturing requirements) are defined for a given structure based on its safety functions and the consequence of its failure on safety classified components or on potential release of radioactive material.

This design aspect is set out in more details in Sub-chapter 3.2.

1.2.6. Design tools

1.2.6.1. Probabilistic Safety Analysis (PSA)

Probabilistic Safety Analysis, PSA, is an essential part of EPR safety and design considerations. The PSA is used to develop the reactor design to assess the relative advantages of different design options within the original project objectives. To be as representative as possible, the PSA also incorporates human reliability assessment, using simplified methods. It also uses component reliability data from French and German or international (EG&G) operating experience and of common mode failure values derived from generic data. The PSA has been developed in successive phases, depending on the state of progress of the different design study stages and in particular:

- an initial level-1 PSA quantifying the probabilities of core meltdown for power states, was carried out within the Basic Design phase,

- a second level-1 PSA covering a broader scope which quantifies the probabilities of core meltdown both for power and shutdown states and incorporates the impact of maintenance at power. This assessment was part of the Basic Design optimisation phase,

- as an extension of the level-1 PSA, a level 1+ PSA which quantifies in broad terms the risk of containment failure for the principal degraded plant states.

These results have made it possible both to confirm the acceptability of the overall reactor design and to improve the design of certain safety systems in terms of redundancy and diversity with regards, for example, to power supplies (e.g. for the reactor emergency cooling system) or cooling circuits (e.g. the containment heat removal system, the spent fuel cooling system in the fuel building pool and for reactor makeup water in certain shutdown states).

In addition, the probabilistic approach was used throughout the post-BDOP phase to ensure that the events considered in the overall safety approach were exhaustive and to determine the design basis for the detailed study phase. This made it possible to:

- confirm and supplement the initial schedule of initiating events to be taken into account in the design and to assign them to three categories: transients, incidents or accidents,

- check that the design provides for a balanced spread of risk across the initiating events, by ensuring that there are no dominant sequences contributing to core meltdown frequency,

- re-examine the list of RRC-A (Risk Reduction Category A) conditions and ensure that specific provisions exist enabling core meltdown risk to be reduced,

- assess the "practical elimination" of certain meltdown sequences in the RRC-B (Risk Reduction Category B) group which could lead to large early releases (such as, for example, containment bypass sequences, boron dilution accidents etc.) in addition to the deterministic provisions included to prevent them.

Afterwards, this probabilistic approach was extended to evaluate the frequency of potential radioactive releases from the following sources:

- The reactor core,
- The spent fuel storage pool,
- The spent fuel handling facilities,
- The radioactive waste storage tanks.

As a result and in addition to the level 1 PSA discussed above, the initial probabilistic approach was supplemented by:

- other accident scenarios considered in a probabilistic manner: these included those relating to the spent fuel pool (loss of cooling or fast draining).
- a level 2 PSA allowing evaluation of the nature, the magnitude and the frequency of radioactive releases outside the containment boundary.
- a level 3 PSA allowing assessment of the risk to the public off-site, frequency vs consequences, associated with radioactive releases.

The initiating events studied include internal transients or hazards originating inside the facility or external hazards, associated with the various plant operational states (i.e. full power, low power, shutdown states).

All aspects of probabilistic studies for the UK EPR (databases, methods, updated calculations and results, incorporating in particular an initial assessment of the proportion of hazards in total core meltdown risk) are presented in Chapter 15.

1.2.6.2. Codes and standards implemented for design

The codes and standards implemented for design, manufacturing and commissioning of the EPR are of three types:

- design codes applicable to French NPPs known as RCCs (Design & Construction Rules) outlining industrial practice for currently operating EDF reactors, which are partially applicable to the EPR,
- EPR design codes known as ETCs (EPR Technical Codes) which set out industrial practices specific to the EPR, and which replace existing RCCs,
- other codes and standards, in the context of the EPR European background (at both regulatory and industrial level).

The RCC and ETC nuclear design codes have been established over the past 20 years to codify French industrial practice and incorporate experience from manufacture, inspection and operation of French nuclear units. The Technical codes incorporate and extend international standards to include subjects which are not yet covered or where existing standards do not allow adequately for the specific requirements of the nuclear industry.

The development of the RCC codes used for the EPR is carried out within the AFCEN organisation, which was created in 1980 to develop French Nuclear Codes and Standards for different types of plant. AFCEN is formed from representatives from AREVA or EDF and other user organisations e.g. CEA, TECHNICATOM, DCN. Requests for interpretation or modifications may be proposed by all the international code users.

The framework for development and maintenance of the EPR design codes, and the experience gained in applying these codes to NPPs in France and internationally, gives confidence in the integrity of the EPR design.

The list of the different applicable design codes is supplied in Sub-chapter 3.8.

1.2.6.3. Computer codes and models

The design of the EPR systems, equipment and structure uses numerous computer codes and models, in particular related to severe accident scenarios.

Qualification of computer codes incorporates a procedure aimed at justifying the validity of results and stipulating the respective responsibilities of the supplier of the code, the subcontractor (if the support study is carried out under contract) and of EDF with regard to code implementation.

In the PCSR, where computer codes are used specifically for the design of equipment or structures, a code description appears at the end of the relevant chapter, i.e.

- the codes used for civil structures and mechanical design are listed in Appendix 3
- the codes used for reactor core design are listed in Appendix 4,
- the accident study (PCC) codes are listed in Appendix 14A,
- the codes used to study severe accident scenarios appear in Appendix 16A.

1.2.6.4. Commissioning - Design and construction quality

The commissioning phase and associated tests must confirm that the as-built equipment and systems (especially those that are safety-classified) can meet their design requirements, and thus demonstrate that the plant is suitable for commercial operation.

The plant commissioning programme includes pre-operational tests prior to the initial start-up tests.

For the design and construction phases, EDF has set up a management system which serves as a basis for all activities related to design and construction, covering plant safety, quality and environmental compatibility.

This system includes:

- provisions ensuring quality within EDF, its subcontractors and suppliers which are in compliance with French regulatory requirements (the quality decree of August 1984) and requirements of ISO 9001 and ISO 14001 standards.

- a general organisation of resources and responsibilities which make it possible to carry out and meet all tasks and actions needed for plant design and construction.

  A description of the quality and project management arrangements for the GDA is given in Chapter 21.

1.2.7. Environmental impact

Environmental impact is considered in this sub-chapter with respect to:

- non-nuclear risks constituted by the installation referred to as "conventional risks",

- normal operating situations such as waste treatment and end-of-life of the reactor (dismantling operations).

The impact of nuclear accidents on the environment is examined in Chapters 14, 15 and 16, as part of the assessment of radiological consequences.

1.2.7.1. Conventional risks of non-nuclear origin

The safety analysis demonstrates that all potential conventional (i.e. non nuclear) risks have been identified and dealt with, and that their consequences are acceptable for the environment, more specifically for the population located near the site boundary. It is based on the following stages:

- preparation of an inventory of equipment which potentially presents a conventional risk,

- identification of those events liable to lead to consequences on the environment or on other site equipment, the risk of which is not eliminated by design provisions,

- following the identification of initiating events, definition of relevant global scenarios and implementation of (physical or administrative) lines of defence for equipment failures which might lead to off-site impacts or adverse consequences on safety functions,

- confirmation of the efficiency of these lines of defence by study of global scenarios.

  This design aspect is set out in Sub-chapter 13.2 for the potential impacts on the safety functions and in Sub-chapter 3.7 more particularly on the off-site impacts.

1.2.7.2. Liquid and gaseous waste

Waste treatment systems contribute to containment, monitoring and control of liquid and gaseous radioactive releases into the environment.

The aim is to significantly reduce liquid and gaseous releases for a given reactor power, in comparison to previous types of reactors (except for tritium and C14).

The systems concerned are as follows:

- The RPE [NVDS] (nuclear island vent and drain) which selectively collects all the liquid or gaseous waste produced inside and outside the containment and channels it to the associated storage and treatment plants. As a consequence this system contributes towards compliance with radioactivity criteria for liquid and gaseous releases.

- The TEP [CSTS] (coolant storage and treatment system) which enables storage, control and treatment of hydrogenated primary liquid waste. This waste is recycled in the primary coolant system to reduce the amount of radioactive waste discharge. It is also used to treat aerated waste produced when the primary system is opened or drained.

- The RCV [CVCS] (chemical and volume control system) which, during the shutdown transient, ensures high flow rate purification of the primary coolant, so as to minimise the doses to operational staff during shutdown and to satisfy radiological criteria specified for the last stages of cold shutdown.

- The TEG [GWPS] (gaseous waste processing system) which contains, treats and enables decay of hydrogenated and aerated gaseous waste derived from treatment of primary coolant or from the gas blanket of primary coolant tanks. Purification of excess gaseous waste produced during plant transients (start-up, shutdown, primary oxygenation) is carried out in series-mounted activated charcoal beds.

  This design aspect is set out in Chapter 11.

1.2.7.3. Solid waste

Reducing waste production from fuel, and in particular "long-lived" waste, is a major element in environmental optimisation of the nuclear fuel cycle, regardless of the ultimate method of management of this type of waste.

The EPR design and performance directly assist in fulfilling this objective. When compared to existing power plants, the EPR offers:

- improved overall use of fuel material as a result of enhanced operating and safety margins as well as increased neutron efficiency. Less nuclear fuel is needed for an equivalent power, with improved possibilities of recycling. Hence, the EPR design enables reductions in natural uranium consumption and in the production of radioactive waste.

- optimisation of recycling and medium-term plutonium management by increasing burn-up levels and enhancing flexibility which makes it possible to implement different types of MOX or innovative fuels.

Implementing high burn-up fuel cycles enables savings of approximately 17% in natural uranium resources, compared to current management systems for a given reactor power.

The result is a 26% reduction in long-lived waste.

With regards to solid waste other than fuel, estimates have been made by considering the best performing 25% of plants in the current French fleet for each type of waste, which give a total volume of approximately 80 m^3/year (in comparison to 120 m^3 which is the accumulated fleet average for 2004). These ambitious estimates are based on improvements in design enabling enhanced selective sorting of waste and, from the very beginning of operations, introducing waste zoning and a policy of radiological cleanliness of the different plant buildings.

This design aspect is set out in Sub-chapter 11.3.

1.2.7.4. Decommissioning

Integration of decommissioning operations into the EPR design has been achieved by:

- anticipating the decommissioning process by simulating activation of materials and postulating potential events conducive to the spread of contamination (via definition of cleanliness and waste zoning at the design stage),
- taking operational feedback into account from sites with large component maintenance,
- choosing materials which make it possible to reduce system activation and the volume of radioactive waste, enhancing the strength of materials for fuel cladding and improving the resistance of the primary cooling system to corrosion and erosion,
- developing construction techniques aimed at facilitating dismantling and removal of contaminated equipment and structures, and enabling the use of shields,
- developing system-related provisions which make it possible to avoid radioactive deposits, restrict the spread of contamination and facilitate decontamination of rooms and equipment,

The design and layout will facilitate decommissioning operations and handling and removal of contaminated structures and equipment. Moreover it will allow the use of biological shielding, facilitate the decontamination of rooms and equipment, and avoid the spread of contamination. Knowledge gained from maintenance and/or replacement operations on large components is taken into account.

This design aspect is set out in Chapter 20.

2. TECHNICAL GUIDELINES

2.1. ORIGIN OF THE TECHNICAL GUIDELINES

The French and German safety authorities as well as the major French and German utilities had early involvement in the definition and review of the EPR development goals.

IPSN and GRS jointly developed a "Proposal for a Common Safety Approach for Future PWRs”, which was endorsed in 1993 by the French and German nuclear reactor advisory committees (GPR and RSK). This proposal was then approved by the French and German nuclear safety authorities (ASN and BMU) in a joint declaration issued to the EPR design project.

Later, French and German Safety Authorities and safety experts worked closely together during the EPR basic design phase, and actively and intensively reviewed the EPR safety concepts on the basis of the above proposal. This review enabled the nuclear safety authorities to influence the design at an early stage of the project.

This work was concluded in October 2000 with the endorsement of the GPR, (with the participation of German experts), of "Technical guidelines for the design and construction of the new generation of pressurised water reactors" (TGs) (see Sub-chapter 3.1 - Table 1).

2.2. ROLE OF THE TECHNICAL GUIDELINES

The TGs present the safety philosophy and approach and general safety requirements that the GPR and German experts considered to be appropriate for the design and construction of the next generation of PWR nuclear power plants to be built at the beginning of the 21st century.

The TGs provide the designer with the views of the Safety Authority on the general safety approach and principles to be applied such as:

- development of new plant designs using an "evolutionary" approach starting from the design of existing plants, taking into account operating experience and analyses already performed for currently operating NPPs,

- introduction of innovative features, in particular for prevention and mitigation of severe accidents.

When design approval for the EPR was issued by the French government in September 2004, the TGs were included as an appendix of the approval letter which confirmed that, at this stage of the EPR project review, the safety options defined by the TGs were considered to be sufficient to meet the established objective of achieving a general safety improvement.

The TGs were used as safety guidelines for the assessment of the EPR safety case. Authorisation for construction of the first French EPR (Flamanville 3) was granted in April 2007, after a review of the Preliminary Safety Analysis Report.

However, since these Technical Guidelines were published, the UK EPR safety case has been developed over the period 2007 to 2012 to take into account specific requirements to meet UK regulatory expectations through the Generic Design Assessment of the UK EPR. As a result, certain guidelines in Sub-chapter 3.1 - Table 1 are either no longer applicable or only partially applicable. For example, section F.1.2.1, which addresses failure of mechanical classified pipes, vessels, tanks, pumps and valves, is superseded by section 3.2 of Sub-chapter 13.2.

3. SUPPLEMENTARY SAFETY DESIGN OBJECTIVES FOR UK EPR

In order to show compliance with UK statutory requirements and regulatory practices for Nuclear Installations, a number of additional design safety objectives are adopted for the UK EPR. Demonstration that these design objectives are met will confirm that the EPR design complies with key HSE Safety Assessment Principles [Ref-1] and other UK regulations.

3.1. FUNDAMENTAL REQUIREMENT OF ALARP

To meet the requirements of UK Health and Safety legislation it is necessary to show that the radiation doses to workers and the general public due to EPR operation, taking into account the possibility of accidents, will be as low as reasonably practicable (ALARP). This requires that all reasonable measures are taken in the design, construction and operation of the plant to minimise the radiation dose received by workers and the general public, unless such measures involve disproportionate cost. To confirm this requirement the following safety design objective is adopted:

SDO-1 The radiation doses to workers and the general public from an EPR, under normal operating and postulated accident conditions, must be as low as reasonable practicable.

Compliance with the ALARP objective, in respect of the EPR design, is demonstrated in Chapter 17.

3.2. DOSES TO OPERATORS AND MEMBERS OF THE PUBLIC IN NORMAL REACTOR OPERATION

The following objectives are adopted for radiation doses to operators and members of the public.

3.2.1. Doses to workers – normal operation

Doses to workers during normal operation of the plant will not exceed UK statutory limits as stated in the Ionising Radiation Regulations (IRR) (1999) [Ref-1], summarised below.

IRR (1999) Dose Limits for employees aged 18 years and over		
Annual equivalent dose limit		
Whole body	**Hands, forearms, feet, arms, skin**	**Lens of eye**
20 mSv	500 mSv	150 mSv

In addition to the above statutory requirement, the following more stringent safety design objective is adopted for normal operation, in order to comply with Target 2 in the HSE Safety Assessment Principles:

SDO-2 The annual whole body equivalent radiation dose to any worker due to normal operation of the EPR shall not exceed 10mSv.

Compliance with this objective is demonstrated in Sub-chapter 12.4.

3.2.2. Doses to members of the public – normal operation

For persons off-site, the radiation dose must not exceed UK legal limits for the doses to members of the public, prescribed in the Ionising Radiation Regulations (1999) [Ref-1], as stated in the table below:

IRR (1999) Dose Limits for other persons		
Annual equivalent dose limit		
Whole body	**Hands, forearms, feet, arms, skin**	**Lens of eye**
1 mSv	50 mSv	15 mSv

The following more restrictive requirement is adopted as a safety design objective for the UK EPR, consistent with the more recent Radioactive Substances Direction 2000 [Ref-2]:

SDO-3 The maximum dose to an individual off-site due to normal operation of an EPR shall not exceed 0.3 mSv and shall not exceed 0.5 mSv for the total site containing the EPR.

In addition, the annual collective radiation dose to persons off-site due to normal plant operation shall be as low as reasonably practicable.

Compliance with this objective is demonstrated in the Pre-Construction Environmental Report (PCER).

3.3. DOSES TO WORKERS AND MEMBERS OF THE PUBLIC DUE TO ACCIDENTS

3.3.1. Doses to workers – accidents

To comply with Target 5 in the HSE SAPs [Ref-1], the following safety design objective is adopted for the UK EPR:

SDO-4 The risk of individual worker fatality due to exposure to radiation from accidents will be below 10^{-6}/yr.

Compliance with this principle is demonstrated in Chapters 12 and 17.

3.3.2. Doses to members of the public off-site – accidents

To comply with Target 7 in the HSE SAPs [Ref-1], the following safety design objective is adopted for the UK EPR:

SDO-5 The risk of fatality of any person off-site due to exposure to radiation from accidents will be below 10^{-6}/yr.

To confirm compliance with Target 8 in the HSE SAPs [Ref-1], the summated frequency of accidents in the UK EPR leading to individual doses of different magnitudes will be assessed against the limits given in the table below.

Effective Dose (mSv)	Total Frequency (Per Year)	
	Broadly Acceptable Limit	Maximum Tolerable Limit
0.1 - 1.0	10^{-2}	1
1.0 – 10	10^{-3}	10^{-1}
10 – 100	10^{-4}	10^{-2}
100 – 1000	10^{-5}	10^{-3}
>1000	10^{-6}	10^{-4}

Table for SDO-6

The following safety design objective is then specified for the accident risk:

SDO-6 The EPR design will ensure that the total frequency of accidents in each of the different dose categories in the above table is below the Maximum Tolerable Limit. The design objective will be to achieve an accident frequency in each dose category that is below the Broadly Acceptable level.

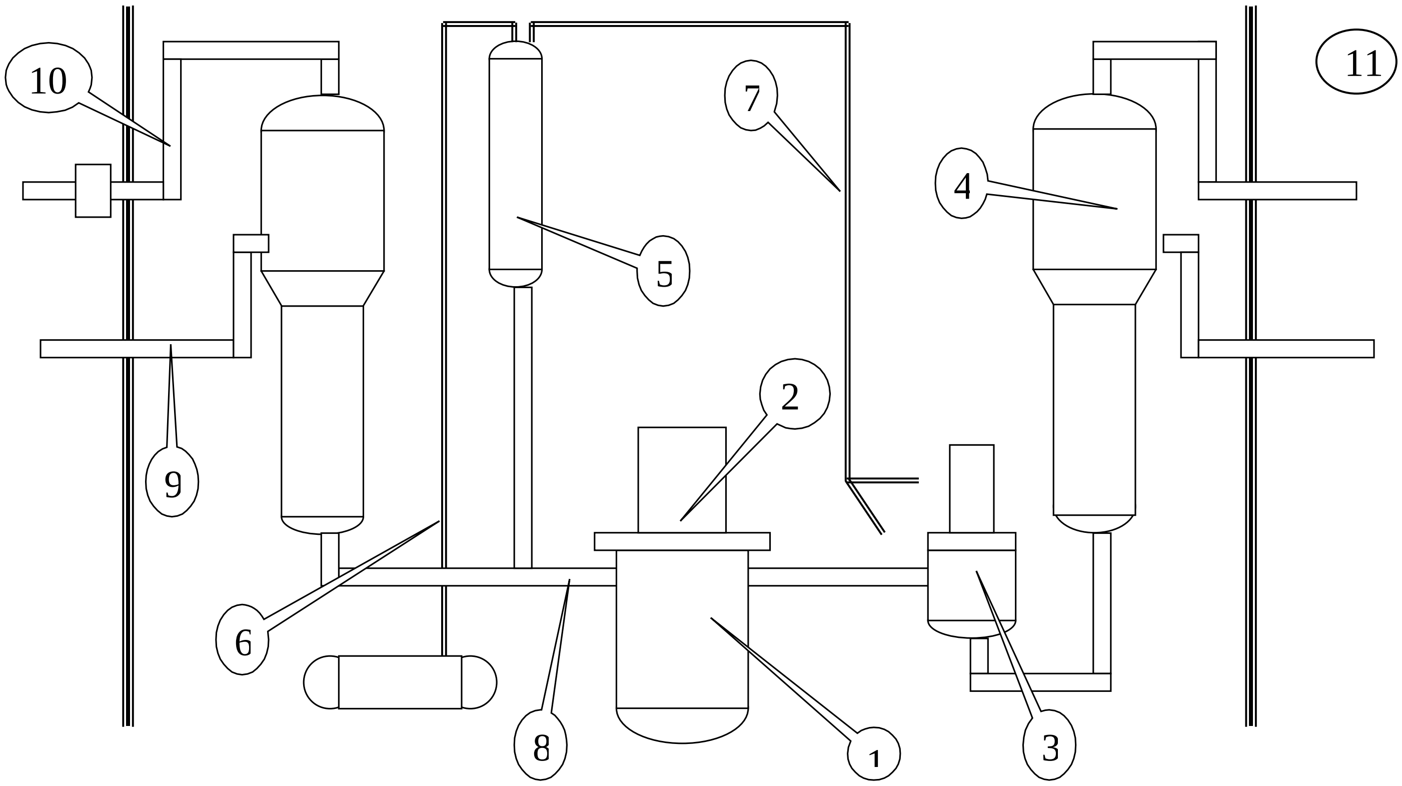
Compliance with this objective is demonstrated in Chapter 15 and Sub-chapter 17.4.

Target 9 in the HSE SAPs proposes limits on societal risk due to potential accidents in a UK nuclear installation, expressed as a risk of occurrence of more than 100 fatalities. To comply with this target the following Safety Design Objective is adopted for the UK EPR:

SDO-7 The total risk of 100 or more fatalities, either immediate or delayed, from on-site accidents that result in exposure to ionising radiation, will be below 10^{-7}/yr.

SUB-CHAPTER 3.1 - FIGURE 1

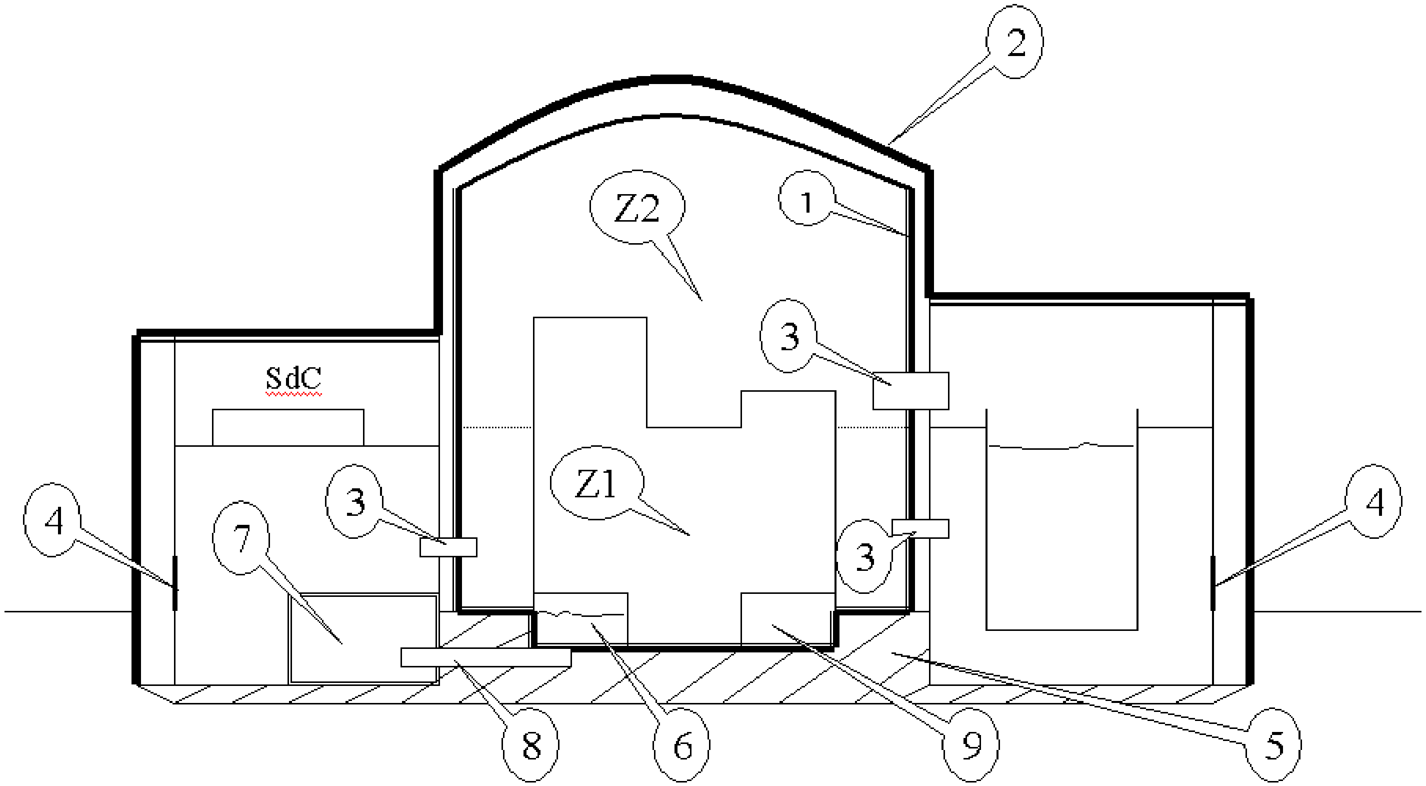
Schematic Diagram of the EPR Main Primary and Secondary Systems



① Reactor Pressure Vessel
② Vessel head
③ Primary Coolant Pump
④ Steam Generator
⑤ Pressuriser
⑥ Discharge of the pressuriser to the relief tank
⑦ Severe Accident Relief Line
⑧ Main Reactor Coolant loops
⑨ SG feed-water system
⑩ Part of the Secondary Cooling System where the HIC claim is applied
Compact Steam System

SUB-CHAPTER 3.1 - FIGURE 2

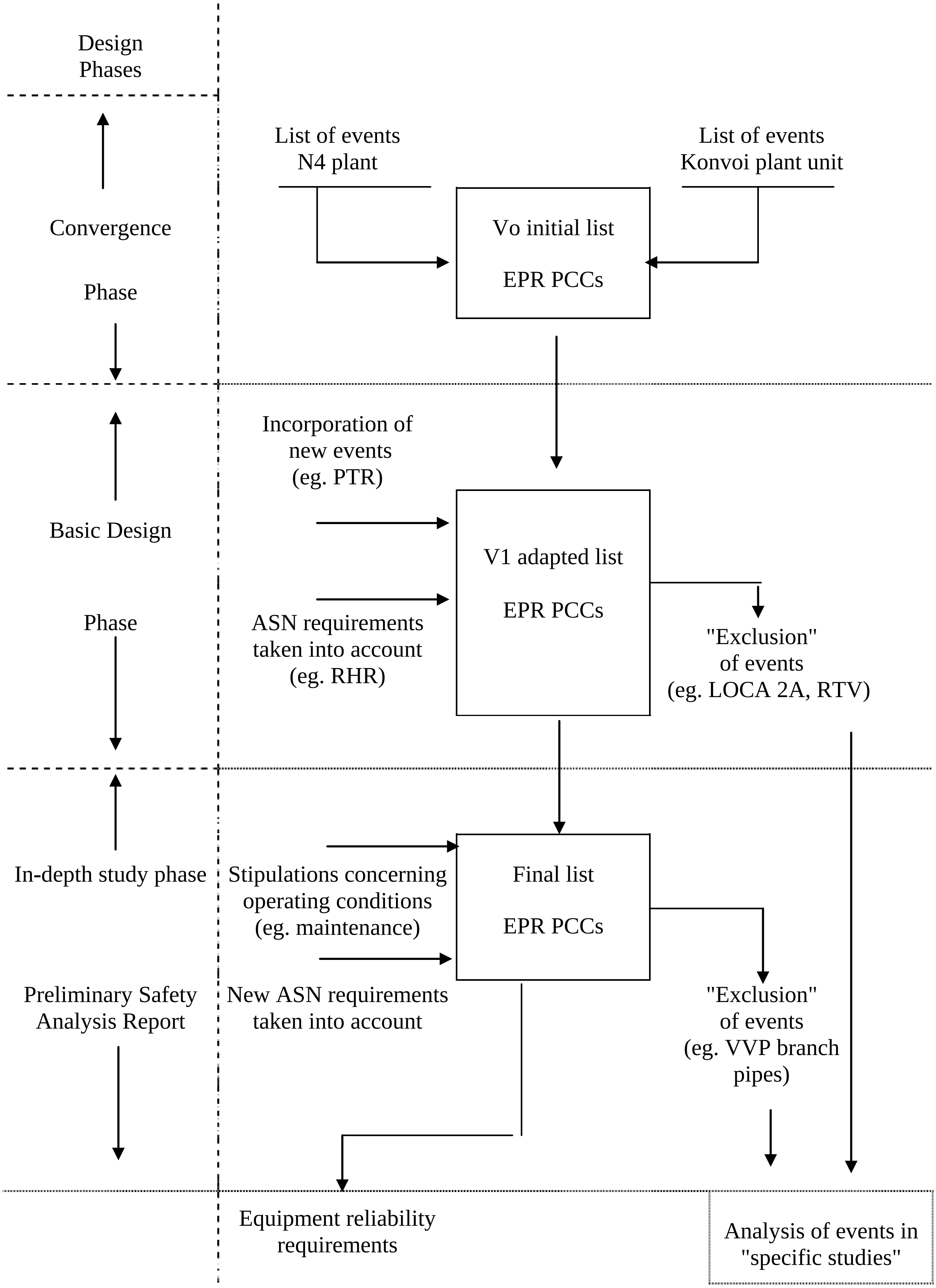
Schematic Drawing of EPR Containment – Reactor Building and Connecting Buildings



- ① Inner Containment
- ② Outer Containment
- ③ Containment Penetrations
- ④ Exterior walls of FB and SB 1&2 protected by the air crash shell
- ⑤ Raft Foundation
- ⑥ IRWST
- ⑦ Safeguard Building
- ⑧ Sumps
- ⑨ Recovering and spreading of Corium System

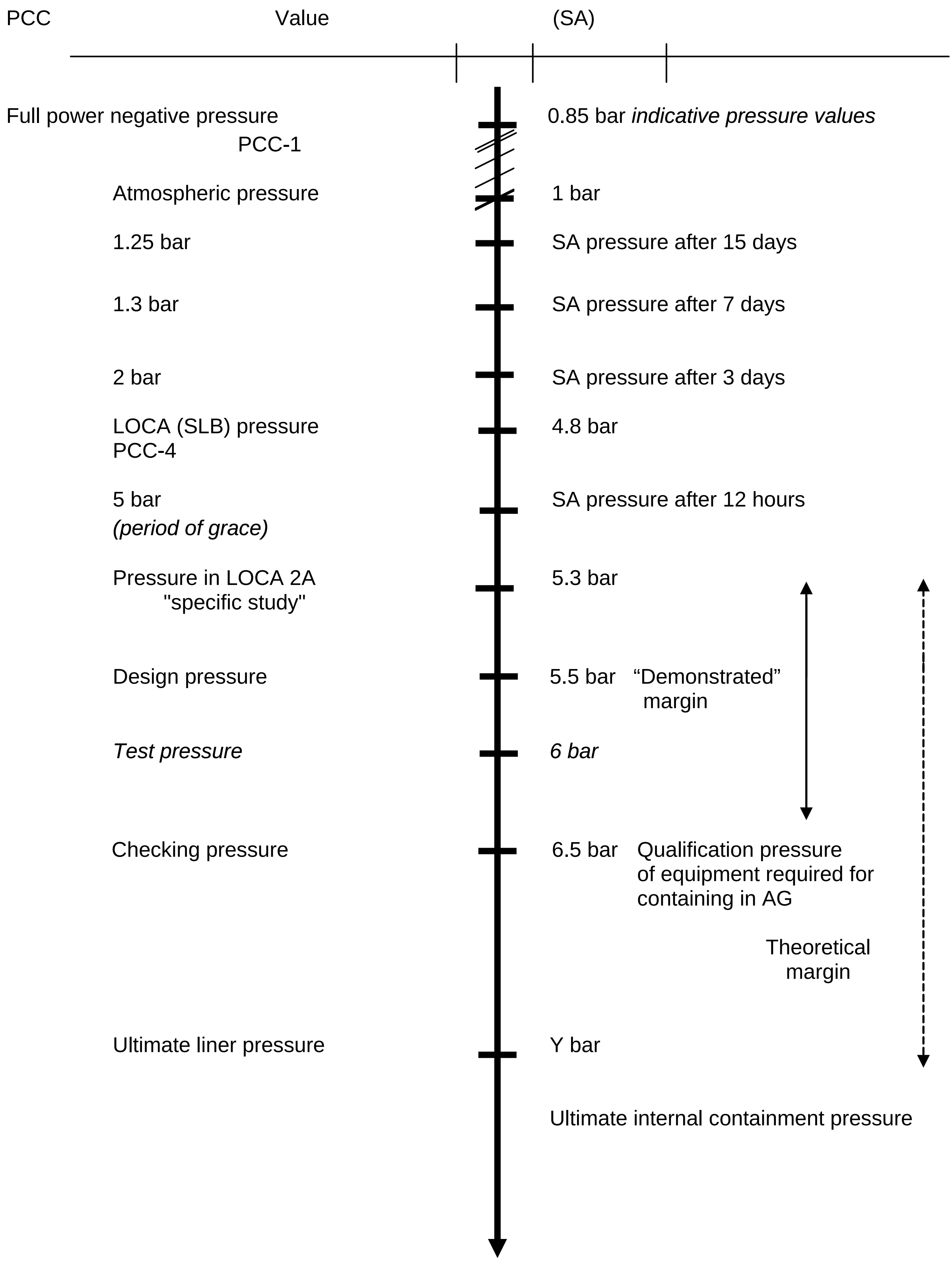
SUB-CHAPTER 3.1 - FIGURE 3

Process for Establishing the List of Initiating Events (PCC-2 to PCC-4)



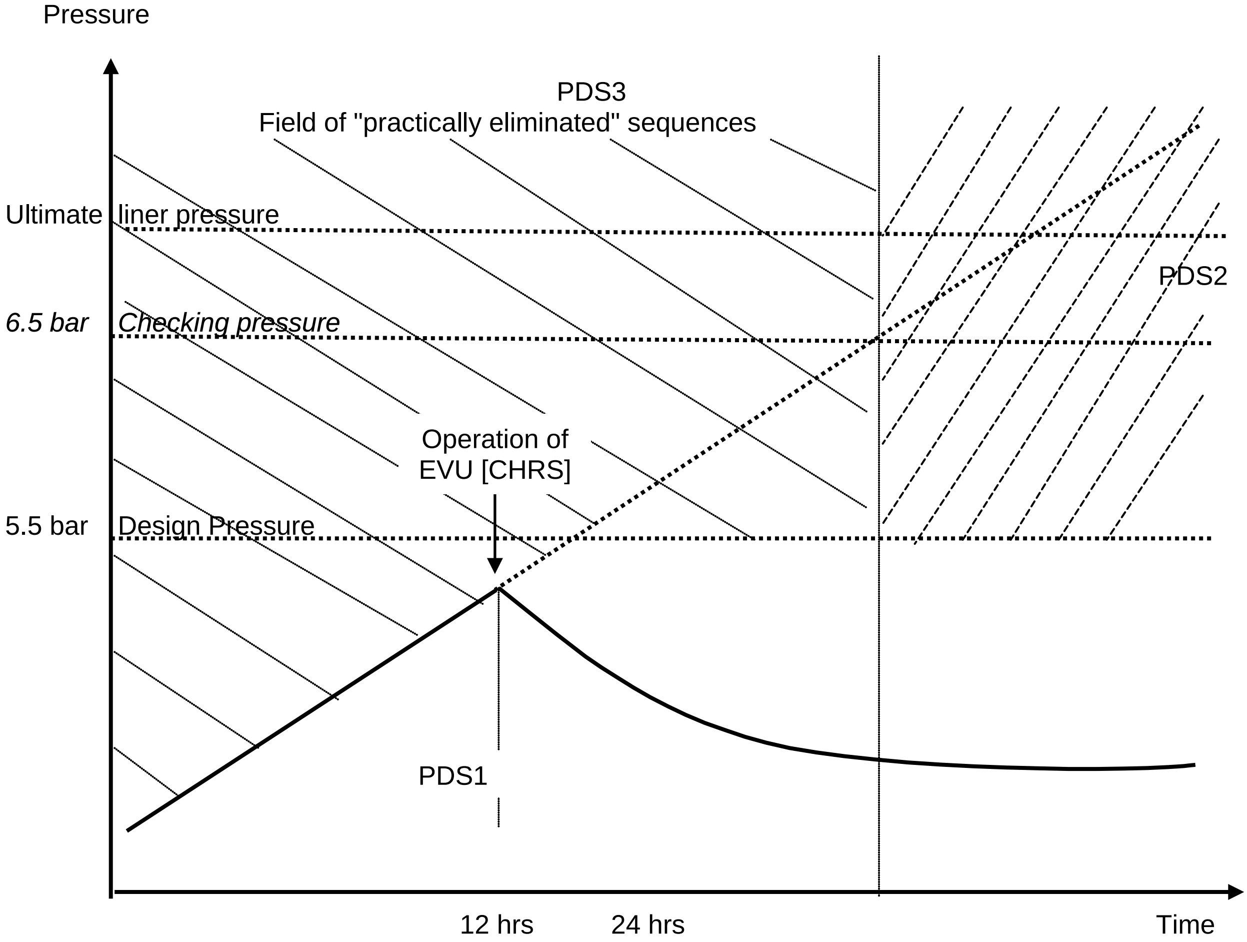
SUB-CHAPTER 3.1 - FIGURE 4

Main Data in terms of EPR Containment Pressure



SUB-CHAPTER 3.1 - FIGURE 5

Principle for dividing up Serious Accident Sequences



Solid line : increase of the pressure in case of low pressure core meltdown - interrupted after operating EVU [CHRS] (not before 12 hours)

PDS 1: sequences with integral containment

PDS 2: sequences leading to delayed containment loss

PDS 3: sequences leading to early containment loss

SUB-CHAPTER 3.1 - TABLE 1

Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurised Water Reactors

Adopted during the GPR/German experts plenary meetings held on October 19th and 26th 2000 [Ref-1]

- - - NOTE - - -

Since the Technical Guidelines were published, the UK EPR safety case has been developed over the period 2007 to 2012 to take into account specific requirements to meet UK regulatory expectations through the Generic Design Assessment of the UK EPR.

As a result, <u>certain guidelines are either no longer applicable or only partially applicable in UK EPR context</u>.

- - - NOTE - - -

SUB-CHAPTER 3.1 – REFERENCES

External references are identified within this sub-chapter by the text [Ref-1], [Ref-2], etc at the appropriate point within the sub-chapter. These references are listed here under the heading of the section or sub-section in which they are quoted.

1. OBJECTIVES AND SAFETY PRINCIPLES

1.1. INTRODUCTION

1.1.2. Overall objectives

[Ref-1] Safety of Nuclear Power Plants: Design (Requirements for Design). ISSN 1020-525X IAEA Safety Standards Series N° NS-R-1. IAEA. 2000. (E)

1.2. THE EPR SAFETY AND DESIGN APPROACH

[Ref-1] Joint declaration of the French and German Authorities on a common safety approach for future pressurized water reactors. DSIN letter no. 1321/93. 2 September 1993.

[Ref-2] Conceptual Safety Features Review File (CSFRF). EPR-CSFRF - 08/93; report jointly prepared by EdF. German Utilities. NPI. Siemens. Framatome. (E)

[Ref-3] Basic Design Report. Report Jointly prepared by Electricite De France, German Utilities. Framatome. Siemens AG. Nuclear Power International. Issue October 1997. (E)

[Ref-4] Basic Design Report. Report Jointly prepared by Electricite De France. German Utilities. Framatome. Siemens AG. Nuclear Power International. Issue February 1999. (E)

[Ref-5] Option de sûreté du projet de réacteur EPR.
[Safety options for the EPR reactor project].
Letter DGSNR/SD2/n°0729/2004. 28 September 2004.

1.2.3. Design scope

1.2.3.1. Internal faults Design Basis Analysis

[Ref-1] T Bruyères. UK EPR Generic Design Assessment Fault and Protection Schedule. NEPS-F DC 400 Revision B. AREVA. February 2011. (E)

1.2.3.5. Hazards analysis

1.2.3.5.1. Hazard identification for the EPR design

[Ref-1] EPR – External hazards – Inventory of combined events with internal faults and/or other (internal and external) hazards taken into account in design.
ENSNEA080058 Revision A. EDF. November 2008. (E)

ENSNEA080058 Revision A is the English translation of ENSNEA050062 Revision A.

1.2.3.5.5. Multiple hazards

[Ref-1] Rapport sur l'inondation du site du Blayais survenu le 27 décembre 1999, rapport IPSN.
[Report on the flooding at Blayais site which occurred on 27 December 1999, IPSN report].
January 2000.

1.2.5. Safety functions, safety classification and associated requirements

[Ref-1] Safety Assessment Principles for Nuclear Facilities. 2006 Edition Revision 1. UK Health and Safety Executive (HSE). January 2008. (E)

3. SUPPLEMENTARY SAFETY DESIGN OBJECTIVES FOR UK EPR

[Ref-1] Safety Assessment Principles for Nuclear Facilities. 2006 Edition Revision 1. UK Health and Safety Executive (HSE). January 2008. (E)

3.2. DOSES TO OPERATORS AND MEMBERS OF THE PUBLIC IN NORMAL REACTOR OPERATION

3.2.1. Doses to workers – normal operation

[Ref-1] The Ionising Radiations Regulations 1999, Statutory Instrument 1999 No. 3232.
HM Stationery Office. ISBN 0 11 085614 7. (E)

3.2.2. Doses to members of the public – normal operation

[Ref-1] The Ionising Radiations Regulations 1999, Statutory Instrument 1999 No. 3232.
HM Stationery Office. ISBN 0 11 085614 7. (E)

[Ref-2] Radioactive Substances (Basic Safety Standards) (England and Wales) Direction 2000. (E)

3.3. DOSES TO WORKERS AND MEMBERS OF THE PUBLIC DUE TO ACCIDENTS

3.3.1. Doses to workers – accidents

[Ref-1] Safety Assessment Principles for Nuclear Facilities. 2006 Edition Revision 1. UK Health and Safety Executive (HSE). January 2008. (E)

3.3.2. Doses to members of the public off-site – accidents

[Ref-1] Safety Assessment Principles for Nuclear Facilities. 2006 Edition Revision 1. UK Health and Safety Executive (HSE). January 2008. (E)

SUB-CHAPTER 3.1 - TABLE1

[Ref-1] Technical Guidelines for the design and construction of the next generation of nuclear pressurized water plant units, adopted during plenary meetings of the GPR and German experts on the 19 and 26 October 2000. (E)