UK EPR	Title: PCSR – Sub-chapter 13.2 – Internal Hazards Protection
	UKEPR-0002-132 Issue 05

Total number of pages: 107	Page No.: I / VI
Chapter Pilot: F. FIORAVANTI (pp.V.JUST) *Name/Initials* *Date 30-10-2012*	
Approved for EDF by: A. MARECHAL *Name/Initials* A.Je.Mareld *Date 31-10-2012*	Approved for AREVA by: G. CRAIG *Name/Initials* G Craig *Date 31-10-2012*

REVISION HISTORY

Issue	Description	Date
00	First issue for INSA review	14-01-2008
01	Integration of technical, co-applicant and INSA review comments	28-04-2008
02	PCSR June 2009 update: - Inclusion of references - Section 1.1: Definition of internal hazards improved. References added to EMI hazard and hazards due to explosive and toxic materials stored on site - Section 1.3.2: Exception to single failure principle noted in case of fire in MCR and justification given - Table 1: previously omitted systems added to table - Section 2.1.1.1.3: Improved explanation and justification given of 2% criterion - Section 4.2.2.1: Arguments given on how integrity claims on reactor coolant pump flywheel are justified, justifying why missile risk from flywheel disintegration is discounted - Section 8.1: Description added of internal flooding events treated in Sub-chapter 13.1.	27-06-2009

03	Consolidated Step 4 PCSR update:
	- Minor editorial changes
	- Update of references to English translations
	- Changes following Step 4 assessment:
	  - introduction of High Integrity Components (section 2);
	  - restructuring of section 2.4 on "Break preclusion for high energy pipework";
	  - introduction of a section 2.5 dedicated to the "Exclusion of leak or break in moderate energy pipework";
	  - modifications regarding protection against missiles (section 4);
	  - addition of text regarding door monitoring system (section 7).
		27-03-2011

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 and typographical changes - Clarification of text (§1.2.4.4, §2.2.2.1.2, §2.2.3, §2.2.4.2, §3.1.2.1, §4.1.2, §4.2.2) - Addition of methodology and principles for the Hazard Fault Schedule (§1.3.1 and new Appendix 1), with reference to an example of a representative Hazard Fault Schedule. - Inclusion of information from the FA3 Validation and Verification Studies for: HEPB (§2.3), missiles (§4.2), cable tray routing (§7.4) and internal flooding (§8.2) - Addition of references to substantiate claims associated with the preclusion of missile generation from failure of RCC-M components not designated as High Integrity Components (HIC) (§4.2.2.1.1) - Substantiation and analysis of the consequences of dropped loads and impact from lifting equipment (§5.3): new sub-section headings 5.3.1 and 5.3.2, addition of reference to the Civil works methodology and addition of text with references to the safety analyses performed for the RS1 and RS2 lifting equipment - Internal flooding (§8.2): addition of text under heading "Step 1: division segregation verification" to substantiate the internal flooding safety case with supporting references	05/09/2012
05	Consolidated PCSR update: - Minor editorial and typographical changes - Update of references (§4.2.2.1.1) - Addition of references (§2.1.2.1, §2.2.1, §3.2.1, §4.1.1, §4.2.2.1.4) - Update of definitions and addition of reference (§2.2.1) - Update of text to refer to HIC rather than break preclusion (§2.2.2.1.2, §2.2.2.1.3, §2.3.1.5, Section 13.2.2 – Table 2, §3.2.1, §4.2.2.1.4, §4.2.3.2.3, §6.1.2) - Update of text regarding failure assumptions for DN>50 classified moderate energy pipework (§2.2.3) - Previous sections 2.4 and 2.5 covering Break Preclusion Break for High and Moderate Energy Pipework deleted - Update of text regarding RCCA ejection consistent with PCC assumptions (§4.2.2.1.3)	31-10-2012

Continued on next page

REVISION HISTORY (Cont'd)

Issue	Description	Date
05 cont'd	Consolidated PCSR update (cont'd): - Addition of references to further human factors studies (§5.3.1, § 5.3.2) - Clarification of text (§8.1.1, §8.1.3.1.1) - Addition of text regarding failure assumptions (§8.1.3.2) - Paragraphs added on "divisional segregation verification" with references to human factors analysis and ALARP study (§8.2)	

For information address:

AREVA NP SAS
Tour AREVA
92084 Paris La Défense Cedex
France

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

TABLE OF CONTENTS

SUB-CHAPTER 13.2 – INTERNAL HAZARDS PROTECTION

The overall design approach for both internal and external hazards is presented in Sub-chapter 3.1. This sub-chapter presents the details of the design principles applied to the protection against internal hazards.

1. GENERAL PRINCIPLES

1.1. LIST OF INTERNAL HAZARDS AND CONTENTS OF SUB-CHAPTER

Internal hazards are events within the site boundary, which have the potential to cause adverse conditions for equipment necessary for fulfilling the three basic safety functions: control of reactivity, removal of heat from the core and containment of radioactive substances. Most of these events originate inside buildings housing this equipment. However, as discussed in Sub-chapter 3.7, events originating in other buildings, or outside buildings, within the site boundary, are also considered as internal hazards. Events of this type considered in the present sub-chapter are as follows:

- missile risk is assessed for missiles originating outside such buildings,
- explosion risks from the conventional island and from on site gas storage facilities are taken into account,
- flooding sources in the conventional island, and due to on-site equipment outside buildings, are considered.

At the present stage of the GDA, hazards due to other on-site facilities affecting the EPR unit, and hazards created by the EPR unit affecting other facilities cannot be readily identified. Such risks will be assessed during site specific studies outside GDA.

Protection against the following internal hazards addressed in the EPR design basis is discussed in this sub-chapter in the section indicated below. The justification for the completeness of this list is provided in Sub-chapter 3.1. For each of the hazards, Sub-chapter 13.2 presents the design requirements, the design basis, and the design verification method (the PSA aspects are presented in Chapter 15):

- Protection against pipework leaks and breaks (section 2 of this sub-chapter),
- Protection against failure of tanks, pumps and valves (section 3 of this sub-chapter),
- Protection against internal missiles (section 4 of this sub-chapter),
- Protection against dropped loads (section 5 of this sub-chapter),
- Protection against internal explosions (section 6 of this sub-chapter),
- Protection against fire (section 7 of this sub-chapter),
- Protection against internal flooding (section 8 of this sub-chapter).

Electromagnetic Interference (EMI) is not addressed in the present sub-chapter as it is addressed elsewhere in the PCSR:

- EMI induced by lightning is the design basis for EMI protection design (see Sub-chapter 13.1, section 7)
- electrical and I&C equipment is designed according to immunity requirements as described in related sections (see Sub-chapter 8.4 and Sub-chapter 7.2). The design of portable equipment permitted to be used in the plant operation phase is required to be compatible with the qualified immunity levels.

Hazardous materials are addressed in the following sub-sections of the PCSR/PCER submission:

- explosive materials are addressed in section 6 of this sub-chapter,
- prevention and limitation of noxious substances following a fire are addressed in section 7 of this sub-chapter,
- risks induced by the presence of non-nuclear facilities and human activities on the site are addressed in Sub-chapter 3.7 of the PCSR
- information on the anticipated storage of hazardous materials is presented in PCER Sub-chapter 3.3, section 7, alongside an assessment of the COMAH regulation for a reference EPR site.

Internal hazard protection is provided to ensure that the safety related functions required to meet the safety objectives discussed in Sub-chapter 3.1 are not unacceptably affected as the result of a hazard. The elementary requirements (in cases where protection of main systems against internal hazards listed above is needed) are summarised in Section 13.2.1 - Table 1. These protection requirements are based on the hazard principles discussed in Sub-chapter 3.1 and the sections specific to each hazard in this sub-chapter.

The application of these requirements in the design of the systems is discussed in the relevant chapters of the system design manuals describing the design of these systems.

1.2. GENERAL PRINCIPLES FOR PROTECTION AGAINST INTERNAL HAZARDS – DESIGN BASIS

1.2.1. General rules

The overall objective is to ensure that equipment required to perform the three main safety functions (control of reactivity, cooling and containment), is suitably and adequately protected against the adverse effects of internal hazards.

The design and installation objectives are to ensure that internal hazards:

- do not prevent F1 functions being fulfilled, even if the functions are not required after such an event;
- do not trigger PCC-3/PCC-4 events (i.e. such events must be avoided where reasonably practicable);

- do not jeopardise the divisional separation of safety trains.

As a result of these requirements, it follows that an internal hazard must not adversely affect:

- more than one element of a set of redundant F1 systems;
- the stability/integrity of the:
  - reactor coolant pressure boundary (except in the case of LOCA);
  - reactor internals, including the fuel elements;
  - main steam and feedwater water pressure boundary;
  - fuel pool and its internal structures, including the fuel elements;
  - safety classified buildings and fire barriers;
  - components whose failure is excluded by design (High Integrity Components, see Sub-chapter 3.1).

In general terms, a sufficient number of redundant systems must remain operational to enable a safe shutdown to be achieved.

Less stringent requirements are imposed in the case of internal hazards resulting from RRC-B events (see section 1.2.4.4 below).

The habitability of the Main Control Room must not be impaired by an internal hazard occurring elsewhere in the plant. In the case where the Main Control Room is not habitable, access to the Remote Shutdown Station must be assured. Furthermore, accessibility to perform local actions must also be ensured, if necessary.

1.2.2. Types of buildings

Internal hazards are postulated to occur in two different types of safety classified building. These two types of buildings are:

- Type 1 buildings: buildings which are separated into divisions, for example, the safeguard buildings and diesel generator buildings;
- Type 2 buildings: buildings or parts of buildings, which are not separated into divisions, for example, the Containment building.

Protection against internal hazards is considered in the design of the unit, through layout requirements and/or design provisions against hazard loads. The requirements are adapted for the two different types of buildings described above.

If an internal hazard occurs in a Type 1 building, the design must ensure that consequences of the hazard are limited to the affected division. This means that building structures necessary to prevent the propagation of an internal hazard (e.g. fire, high energy line break, flood) must be designed to withstand the consequences of the internal hazard. This approach also requires the minimisation of inter-connections between the divisions. Propagation of the hazard through divisional inter-connections is prevented by avoiding penetrations in barriers or, where this is not possible, by the use of isolation or decoupling devices.

If an internal hazard occurs in a Type 2 building, the installation rules or the design must ensure that not more than one redundant F1 system is affected. A distinction must be made between local and global effects resulting from the hazard:

- Local effects are effects limited to the immediate area where the hazard occurs, e.g. jet impingement forces, pipe whip effects, fire;

- Global effects are those which may have an impact on larger areas of the building, e.g. an increase in ambient conditions or flooding. Global effects resulting from internal hazards must be confined to the affected building.

1.2.3. Prevention of PCC-3 and PCC-4 events

The design and installation of classified or non-classified mechanical, electrical and control systems must, where reasonably practicable, be such that an internal hazard cannot trigger a PCC-3 or PCC-4 event.

However, it is accepted that internal hazards in the conventional island, in the Level 1 instrumentation and control system, or in the containment building, may trigger a PCC-2 event.

If, in exceptional circumstances, a PCC-3 or PCC-4 event is caused by an internal hazard, an adequate number of safety classified systems/redundancies, designed to mitigate the effects of the PCC-3 or PCC-4 event, must remain operational, taking into account the single failure criterion.

Internal hazards in the nuclear auxiliary building, the turbine hall or other site buildings, which are non safety-classified must be analysed to show that inadmissible consequences to safety-classified buildings are avoided.

1.2.4. Classes of internal hazards – combinations and dependencies

Due to their possible consequential damage including combinations and dependencies, different types of internal hazards are distinguished as follows.

1.2.4.1. Internal hazards independent of PCC-2 to PCC-4 or RRC events

This class of hazard has no impact on the neutronic and thermal-hydraulic behaviour of the core or reactor coolant system, and does not result in radiological consequences. The general analysis rules described within section 1.2.1 of this sub-chapter are applicable to this class of hazard.

1.2.4.2. Internal hazards which could trigger a PCC-2 event

Internal hazards occurring independently of PCCs should not trigger a PCC-3 or PCC-4 event. However, as occurrence of a PCC-2 event cannot be discounted, it must be demonstrated through functional analysis that an adequate number of systems/redundancies remain available to limit the consequences of the hazard, consistent with the assumptions of the transient analysis of the PCC-2 event. Within the context of the internal hazard, it is not necessary to demonstrate that safety criteria have been met as this is implicitly demonstrated by the transient analysis associated with the PCC-2 event.

1.2.4.3. Internal hazards resulting from a PCC-3 or PCC-4 or RRC-A event

For these hazards, the thermal-hydraulic, neutronic and radiological consequences are addressed in the safety analysis of the PCC-3 or PCC-4 or RRC-A events. The rules and criteria applicable to the appropriate PCC-3 or PCC-4 and RRC-A event are applied.

Non-redundant safety classified systems, components or structures must be designed to withstand the impact of internal hazards. In the case of redundant safety classified systems, components or structures, internal hazard induced failure of redundant elements that are not required to achieve a safe state is an acceptable consequence.

1.2.4.4. Internal hazards resulting from RRC-B events

Systems required for the safety demonstration are specially designed to withstand the consequences of internal hazards resulting from RRC-B events (core meltdown accidents). The design against such hazards is based, as far as possible, on realistic assumptions. The single failure criterion is not applied, but the following must be shown:

- the containment remains leaktight;
- where necessary, the containment internal structures maintain their load bearing capability;
- the functionality of the containment function support systems (e.g. hydrogen control system, containment residual heat removal system EVU [CHRS]) and necessary instrumentation is ensured;
- the generation of missiles that could endanger the containment function or its support systems is avoided;
- habitability of the control room is ensured.

By demonstrating the above requirements, it follows that the systems required to control the RRC-B event are not unacceptably affected by the hazard.

1.3. DESIGN VERIFICATION

1.3.1. General considerations

As a general rule, internal hazards are treated in a deterministic way in the design verification. It is noted that for some hazards probabilistic analysis is also performed to complete the safety analysis (see Chapter 15).

The initial conditions considered for analysis are normal operating conditions.

External hazards or other postulated initiating events occurring in combination with an internal hazard are not considered. Also, unlikely combinations of internal hazards and specific initial conditions (e.g. short duration plant states during normal operation) are excluded from the analysis.

In the design verification, an internal hazard is not considered as a single failure. The logic behind this approach is that single failure criterion should not be used to generate scenarios involving a combination of two independent hazards, thereby increasing the severity of the accident scenario analysed.

Internal hazards considered in the analysis (in a specified location) are classified into one of the following four categories. The categories are presented below alongside a description of the approach that is taken the assessment:

Postulated hazard initiating events and their potential consequences will form the basis of a Hazard Fault Schedule for all identified internal and external hazards, to present the Safety Functions considered necessary to maintain nuclear safety during and after their occurrence, deriving the category of function and therefore the class of Structures, Systems and Components (SSCs) required to deliver such a function. The methodology for a representative Hazard Fault Schedule is given in Appendix 1. Sub-chapter 3.2 details the categorisation of Safety Functions and the classification of SSCs.

1.3.1.1. Internal hazards independent of a PCC-2 to PCC-4 or RRC event

A functional analysis is required to demonstrate that it is possible to bring the unit to a safe shutdown state, despite a single failure and preventive maintenance (for most cases, a simple check is performed to show that a sufficient number of safety trains are available).

As there is no PCC-2 to PCC-4 or RRC event, both safety and non-safety classified systems may be considered in the analysis, provided their performance is not impaired by the internal hazard. A single failure can be applied either to a safety or non-safety classified system. Systems or equipment installed to prevent failure of more than one redundant system must be safety classified (at least F2 classified).

1.3.1.2. Internal hazards which could trigger a PCC-2 event

An analysis must be performed to demonstrate that the unit can be returned to a safe state despite an additional single failure and preventive maintenance. For this class of internal hazard, a specific transient analysis is not required as this is provided by the corresponding PCC-2 event analysis.

The analysis of the internal hazard is limited to a functional analysis, which demonstrates that an adequate number of functions remain available to control the PCC-2 event.

1.3.1.3. Internal hazards resulting from a PCC-3 or PCC-4 or RRC-A event

The objective of the analysis for this class of internal hazards is to demonstrate that the boundary conditions used in the analysis of the PCC or RRC-A event are not affected by the hazard. Hence the systems required to control the event are not unacceptably affected.

As an example, LOCA is considered within the context of the PCC-3 or PCC-4 safety analysis. The functional analysis of the associated internal hazard must demonstrate that a LOCA involving one RCS loop does not impair the performance of other loops and that instrumentation and control equipment inside the containment is suitably qualified and protected.

1.3.1.4. Internal hazards resulting from RRC-B events

The objective of the analysis of these types of internal hazards is to demonstrate that the boundary conditions used in the analysis of the RRC-B event are not affected by the hazard.

1.3.2. Application of the single failure criterion

The single failure criterion must be applied deterministically in the analysis of internal hazards which:

- are independent of PCC-2 to PCC-4 or RRC events,
- or can lead to PCC-2 events,
- or are a consequence of PCC-3 or PCC-4 events.

The single failure must be considered for:

- systems which enable a safe state to be reached, or,
- equipment which limits the effects of the hazard inside a division in buildings split into divisions (e.g. valves, dampers), or,
- equipment which limits the effects of the hazard to the affected area in buildings not split into divisions (e.g. valves, dampers), if applicable.

Exception: For functional analysis of a fire in the Main Control Room (MCR), a single failure is not considered for the equipment of the Process Information and Control System (PICS) (see Sub-chapter 7.5). This system is operated from the Remote Shutdown Station (RSS) because the MCR in this event is considered to be unavailable. The frequency for losing the MCR due to a fire is judged to be low (see Sub-chapter 15.2) due to the presence of operating personnel who would be able to extinguish the fire at an early stage, and the adequacy of fire protection measures.

For analysis of internal hazards resulting from RRC-A or RRC-B events, a single failure is not considered.

1.3.3. Rules for operator actions

In the design verification, operator action is not claimed for at least the first 30 minutes following the receipt of the first significant information. For initiation of local manual action by the operator (i.e. action from outside the main control room), operator action cannot be claimed for at least 60 minutes after receipt of the first significant information.

1.3.4. Preventive maintenance

The design verification must take into consideration the preventive maintenance of systems, in accordance with their preventive maintenance programme, i.e. one system train is assumed unavailable during in-service maintenance, or one or more trains are assumed unavailable during shutdown periods, in the following situations:

- Internal hazards independent of a PCC event;

- Internal hazards which could trigger a PCC-2 event;
- Internal hazards resulting from a PCC-3 or PCC-4 event.

For internal hazards resulting from RRC-A or RRC-B events, maintenance states are not considered.

1.3.5. Internal hazards during shutdown periods

Under unit shutdown conditions, the influence of maintenance work on the systems necessary for controlling internal hazards must be analysed if:

- the maintenance work is a potential source of an internal hazard;
- the maintenance work results in reduced availability of these systems.

SECTION 13.2.1 - TABLE 1

Summary of the requirements for protection against internal hazards

	Pipework leaks and breaks	Failures of tanks, pumps and valves	Internal missiles	Dropped load	Internal explosion	Fire	Internal flooding
F1 electrical power supply	Yes	Yes	Yes	Yes	Yes	Yes	Yes
APG [SGBS] (F1 functions)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ARE [MFWS] (F1 functions)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ASG [EFWS]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CFI [CWFS] (F1 functions)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
CRF (F1 function)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DCL	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DEL	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DER (1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DFL	No	No	No	No	No	Yes	No
Emergency diesel generators	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Ultimate diesel generators	No	No	No	No	No	No	No
DMK	No	No	No	Yes	Yes	Yes	Yes
DVD	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DVL	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DVP (F1 functions)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DWB	No	No	No	No	Yes	Yes	Yes
DWK (F1 isolations)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DWL [CSBVS]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DWN	No	No	No	No	No	No	No
DWQ	No	No	No	No	No	No	No
DWW	No	No	No	No	No	No	No
EBA [CSVS] (F1 functions)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
EDE [AVS]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ETY	Yes	Yes	Yes	Yes	Yes	Yes	Yes
EVF	No	No	No	No	No	No	No
EVR [CCVS]	No	No	No	No	No	No	No
EVU [CHRS] (2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
JAC	Yes	Yes	N/A	N/A	N/A	Yes	Yes
JDT [FDS]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
JPI	Yes	Yes	Yes	Yes	Yes	Yes	Yes
JPV	N/A	N/A	Yes	N/A	N/A	Yes	Yes

	Pipework leaks and breaks	Failures of tanks, pumps and valves	Internal missiles	Dropped load	Internal explosion	Fire	Internal flooding
KER [LRMDS]	No	No	No	No	No	No	No
KRT [PRMS] (F1 functions)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PTR [FPPS/FPCS] (3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RBS [EBS]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RCP [RCS]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RCV [CVCS] (F1 functions)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
REA [RBWMS]	No	No	No	No	No	No	No
REN [NSS] (F1 functions)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RES (F1 functions)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RGL [CRDM]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RIC (F1 functions)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RIS [SIS]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RPE [NVDS] (1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RPN	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RRI [CCWS]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SAT (1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SEC [ESWS]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SED (1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SEK [CILWDS]	No	No	No	No	No	No	No
SGH	Yes	Yes	Yes	Yes	Yes	Yes	N/A
SGN (DEA [SSSS] tanks)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SIR (1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNL (1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SRU [UCWS] (2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TEG [GWPS] (1)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
TEP [CSTS]	No	No	No	No	No	No	No
TER [ExLWDS]	No	No	No	No	No	No	No
TES [SWTS]	No	No	No	No	No	No	No
TEU [LWPS]	No	No	No	No	No	No	No
VDA [MSSS]	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VVP [MSSS] (F1 functions)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

NOTES:

N/A: not applicable.

1) Containment Isolation function only.
2) For internal hazards which may result from an RRC-A event, requiring the intervention of this system, or from an RRC-B event.
3) Cooling trains, containment penetrations and drainage pipework isolation.

2. PROTECTION AGAINST PIPEWORK LEAKS AND BREAKS [REF-1]

2.1. SAFETY REQUIREMENTS

2.1.1. Safety objectives

The general safety objectives for internal hazards are given in section 1 of this sub-chapter.

2.1.2. Requirements for protection against failures of pipework

2.1.2.1. Identification of risks

Breaks or leaks in pipework can appear at any time during plant operation; it is therefore important to be able to detect leaks and maintain the plant in a safe state.

In assessing an assumed pipework failure, it is necessary to take into account the various effects of the postulated event in order to estimate the severity of the fault.

The general approach aims at showing that the consequences of gross failure are acceptable. The components for which such justification is not achievable are identified and are submitted to a set of specific requirements in order to justify their high integrity [Ref-1]. The list of these High Integrity Components (HIC) is given in Sub-chapter 3.1.

2.1.2.2. Deterministic and probabilistic objectives

The approach taken for the protection against pipework failure is deterministic.

The overall deterministic objectives are given in section 1 of this sub-chapter.

2.2. DESIGN BASIS

2.2.1. Definitions

<u>High energy components</u>

Components containing water or steam at pressures greater than or equal to 20 bar (absolute), or temperatures greater than or equal to 100°C, under normal plant operating conditions. Components containing gas at a pressure above atmospheric pressure are always considered to be high energy components. All other components are considered to be moderate energy components.

<u>Moderate energy components</u>

Pressurised components not classified as high energy components.

Leak

Stable subcritical through wall crack, or loss of leaktightness of a bolted junction in high or moderate energy pipework.

Break

Circumferential rupture as a result of an unstable circumferential failure.

Gross failure

Complete disruptive failure of a component, including fast fracture with possible missile generation.

High Integrity Component (HIC)

Components whose gross failure is generally not addressed in the current safety analysis, and where, in general, it cannot be justified that the consequences of the failure are acceptable. For these components, a set of specific measures are taken into consideration to achieve and demonstrate their high integrity.

Break preclusion

Concept to preclude failure of pipework[1]. This concept requires additional measures in terms of mitigation [Ref-1].

2.2.2. Failure assumptions for High Energy Pipework

2.2.2.1. High Energy Pipework

2.2.2.1.1. Small diameter pipework (≤ DN 50)

Type and location of breaks

For small diameter pipework (less than or equal to 50 mm nominal bore, (≤ DN 50), there is no restriction in the assumed break location, i.e. breaks are assumed to occur at any place on the pipe.

---

1 *Although the MCL and MSL are designated as HIC for the UK EPR, and the associated requirements are described in Sub-chapter 3.4, additional conservative risk reduction measures, which are inherent to the "Break Preclusion Concept" to explain why the 2A LOCA and the double-ended MSL Break are not considered in the design basis, or why the Surge Line break is the largest LB LOCA considered as a PCC-4 event, are described in Sub-chapters 5.2 and 10.5..*

The HIC claim includes requirements which make up the first 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 simply as an additional conservative measure.

<u>Failure effects</u>

As a result of the relatively low energy potential, secondary effects due to breaks are only analysed with respect to:

- Loss of fluid relating to the function of the safety classified system (loss of pipework function);
- Consequential damage to small diameter pipework or cables (e.g. pressure impulse lines) caused by jet impact forces and pipe whip;
- Consequential damage to electrical and instrumentation and control equipment due to increases in pressure, humidity, temperature and radiation;
- Flooding consequences.

2.2.2.1.2. Pipework (> DN 50)

This section does not apply to pipework covered by the HIC claim (see Sub-chapters 5.2 and 10.5).

Pipework failure effects discussed in section 2.2.4 below are required to be considered for all leaks and breaks in pipework with a nominal bore > 50 mm (> DN 50). Pressure waves inside the ruptured system due to the rapid depressurisation of the fluid are considered. For leaks due to small fractures it is more realistic to consider a steady pressure reduction.

A summary of the failure assumptions assigned to high energy pipework systems is shown in Section 13.2.2 – Table 2.

2.2.2.1.2.1. Leaks and Breaks in classified High Energy Pipework

<u>Type and location of leaks and breaks:</u>

Leaks and breaks in safety classified pipework (see Sub-chapter 3.2) are postulated to occur at the following locations:

- At pipework terminations;
- In quality level 1 pipework (e.g. M1 requirements):
  - o at intermediate locations where the usage factor is higher than 0.1, in combination with a variation magnitude higher than 2.4 Sm (see RCC-M code, Sub-chapter 3.8)), where the variation magnitude is the sum of the primary and secondary stresses between two system conditions (calculated using equation (10) in paragraph B3653 of the RCC-M);
  - o at intermediate locations where the usage factor is lower than 0.1, in combination with a variation magnitude (as described above) higher than 3 Sm and a thermal expansion stress variation magnitude higher than 2.4 Sm. The thermal expansion stress, is based on the sum of the primary stresses and the secondary stress in the membrane, including flexing (outside of thermal flexing and thermal expansion) (equations (12) and (13) of paragraph B3653 of the RCC-M).

- In quality level 2 and 3 pipework (e.g. M2 and M3 requirements):
  - o at intermediate locations where the stress rate exceeds 0.8 (1.2 Sh + SA) (or equations (9) and (10) of NC or ND 3652 of ASME). The stress rate in quality level 2 pipework is calculated by the sum of equations (10) and (7) of paragraphs C3650 of the RCC-M. In quality level 3 pipework, similar stress criteria are applied by using equations (2) and (3) of the EN13480 standard.
  - o If it is not possible to determine an intermediate location using the above approach or if a single break location is defined, two points of maximum stress with a 10% difference in stress intensity (or, if this difference is lower than 10%, with at least one bend between the two) should be chosen. If the pipe is straight, without stress concentrations and if all of the stresses are below the admissible level, only one location where the stresses are at their highest should be chosen.

It must be verified that the leak and break location chosen, represents bounding conditions in relation to the safety functions performed by the equipment located in the room under consideration. If sensitive areas are detected, additional measures must be taken (for example: analysis of the layout, further protection devices).

In the case of a guillotine break, the break size is usually assumed to equal 2A (where A = cross sectional area of the pipe). If movement at the ends of the pipework is limited (for example, by a whip restraint or as a result of pipework stiffness), a smaller and more realistic break size may be chosen.

A guillotine break refers to a break involving complete severance of a pipe.

2.2.2.1.2.2. Leaks and Breaks in non-classified High Energy Pipework

Leaks and breaks in non-safety classified pipework (according to Sub-chapter 3.2), are postulated to occur at varying locations, and the pipework failure effects are considered.

As a principle, the installation of non-classified high energy pipework in safety classified buildings (with the exception of the Nuclear Auxiliary Building) is limited to the minimum extent reasonably practicable.

2.2.2.1.3. Prevention of High Energy Line Breaks and Leaks

If certain specific requirements are adhered to, catastrophic failures of pressurised pipework may be discounted in the deterministic approach used during the design of the equipment and surrounding structures. This concept is based on the following requirements:

a) Break Preclusion

In order to establish that the possibility of a pipe break can be ruled out from the safety assessment, the HIC conditions presented in section 0 of Sub-chapter 3.4, and detailed in Sub-chapters 5.2 and 10.5, must be met.

The HIC claim applies to the Reactor Coolant System pipework (see Sub-chapter 5.2) and to the main steam lines (see Sub-chapter 10.5) between the steam generators and the fixed points downstream of the main steam isolation valves.

b) 2% Criterion [Ref-1]

The 2% criterion is a criterion which allows pipe breaks to be excluded from the design basis if pipework is in operation under high energy conditions for a period of less than 2% of the plant lifetime. The 2% criterion is applicable only to safety classified pipework of more than 50 mm nominal bore, (> DN 50), that is designed in accordance with mechanical codes.

Application of the 2% criterion requires the following conditions to be met:

- Application is restricted to classified pipework (see Chapter 3), for which there is/are:
    - high quality material characteristics, in particular toughness;
    - conservative stress limits;
    - avoidance of stress concentrations through optimum design;
    - assurance that optimised manufacturing and testing technologies have been applied;
    - appropriate consideration of operating fluid characteristics;
- Limited period in which the systems experience high energy mode;
- Negligible likelihood of crack propagation, because of reduced load cycling due to the systems limited operational use in high energy mode, i.e. the number of load cycles is relatively low compared to normally operating systems;
- Good prediction of operating modes and anticipated stress levels, with the degree of fatigue notably being lower than 1;
- Adequate surveillance provisions (e.g. non-destructive testing, pressure testing, integral visual inspections).

The following measures are considered within the context of the in-service inspection and operational surveillance:

<u>1. Integral visual Inspection</u>

Integral visual inspection can be generally performed during plant walk down reviews. These enable the condition of the pipework to be visually assessed (for pipework, the thermal insulation is removed).

Absence of the following should be verified:

- Mechanical damage in general (e.g. bending, breaks, pipe movement);
- Operation of support devices (e.g. free movement of the rollers, mounting positions of standard support devices, operability of spring hangers);
- Indication of leaks;
- Defects in threaded connections, measuring devices and impulse lines;
- Vibrations, noise (e.g. cavitation).

2. Non-Destructive Testing

Internal and external surfaces of the weld area, and base material, that are subject to high stress concentrations (e.g. pipe bends and elbows), may be examined.

The inspection of external surfaces can also be performed using surface crack detection methods (e.g. dye penetrant testing for austenitic steels, magnetic particle inspection for ferritic steels) and volumetric inspection techniques, using ultrasonic and radiographic inspection.

Some of the tests performed for the external surfaces, may not be possible for internal surfaces.

3. Pressure tests

Pressure testing is required for pipework in accordance with design rules, codes and statutory or regulatory requirements.

Independently of these requirements, pressure testing may replace non-destructive testing in specific circumstances, for example, where a high level of radiation exists, or access is restricted.

For the UK EPR the 2% criterion is applied to the following systems only:

The main steam discharge lines downstream of the safety valves/isolation valves
The pressuriser discharge lines
The Emergency Feed Water System (ASG [EFWS]) pipework upstream of the first isolation valve of steam generator

All of the above systems are part of the safeguard systems for accident management. As discussed in sub-section 2.2.2.1.4 below, the 2% criterion is conservatively not applied to Safety Injection System – Heat Removal System (RIS [SIS] / RRA [RHRS]) pipework (even though the service time criterion is met).

The 2% criterion approach, in use in the design of existing French NPPs and is similar to standard US practice (see SRP 3.6.2 [Ref-1], and related Branch Technical Positions (BTPs) [Ref-2] [Ref-3]) and is also recognised in international safety standards (see IAEA Safety Guide [Ref-4]).

Given the conditions for application of the 2% criterion, the probability of break in the pipework in the three systems to which it is applied is considered very low. It should be noted that for the first two systems, guillotine failures, should they occur, would not directly lead to core melt, since the affected pipework is downstream of the discharge valves. As regards the ASG [EFWS], it is considered that the probability of guillotine failure of one line is much lower than the probability of failure of the active components within the line: hence the availability assessment of the system assumed in PSA studies (see Chapter 15) is unaffected by the application of then 2% criterion.

The failure assumptions are shown in Section 13.2.2 - Table 1 below.

2.2.2.1.4. Specific requirements for shutdown conditions

For shutdown conditions, specific consideration is given to systems which are used in high energy mode.

Breaks in pipework less than or equal to 50 mm nominal bore (≤ DN 50), are postulated during conditions B and C (high energy operation) for the Reactor Coolant System (RCP [RCS]) and its connected pipework, up to the second isolation valve, classified as RCC-M category 1.

Beyond the reactor coolant system second isolation valve, the RIS [SIS] / RRA [RHRS] system trains which fulfil the RHR closed loop function, are only considered in high energy mode from a starting temperature of 120°C, until the reactor coolant system pressure falls below 20 bar and the temperature drops below 100°C. The connection temperature for trains 2 and 3 is less than 100°C. Even though the RIS [SIS] / RRA [RHRS] is operated as a high energy system over service periods for less than 2% of the unit service life, the 2% criterion is not applied to RIS [SIS] / RRA [RHRS] pipework. Breaks in the main sections of this pipework (DN 250) are considered at locations inside the containment enclosure and in safeguard buildings 1 to 4 during reactor conditions C and D.

2.2.3. Failure assumptions for Moderate Energy Pipework

For small diameter moderate energy pipework (DN ≤ 50), breaks are postulated with no restriction in the assumed break location, i.e. breaks are assumed to occur anywhere in the pipe.

Leaks are generally postulated for classified moderate energy pipework with mechanical requirements (DN > 50) (see Sub-chapter 3.2). The location of leaks is determined using formulas (7) and (10) of sections C and D 3650 of the RCC-M code [Ref-1] to calculate the pipework stress rates. Leaks are located where stress rates are above or equal to 0.4*(1.2Sh+SA). However, as pipework stress rates are not generally known at the basic design stage, there are no specific assumptions regarding the leak location in the first step of the studies. The leak rate equivalent to section A_L is calculated using the following formula [Ref-2] to [Ref-5]:

$$A_L = \frac{di \times s}{4}$$

Where di: internal pipe diameter

s: thickness of pipe wall

For the divisional segregation verification (see section 8.2, step 1), the internal flooding safety case uses pessimistic failure assumptions (Double Ended Guillotine Break for classified moderate energy pipework with DN > 50). This analysis, which uses realistic assumptions wherever justified, provides a demonstration that divisional segregation is maintained even with the assumption of the most severe flooding event possible in each building.

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

For moderate energy pipework, the effects of leaks and breaks are only to be considered for flooding, radiation risks and the loss of pipe functionality

Moderate energy systems considered in the analysis are, for example, the fire fighting system, the liquid waste treatment system, the condensate extraction system, etc.

2.2.4. Protection against pipework failure effects

A summary of the pipework failure effects is provided in Section 13.2.2 - Table 3 below.

During the design of the safety classified structures and mechanical, electrical and instrumentation and control system components, the effects of the following on the consequences of leaks and breaks are to be considered.

For high energy pipework:

- Jet impingement forces.
- Pipe whip.
- Reaction forces.
- Compression wave forces.
- Flow forces.
- Differential pressure forces.
- Pressure build-up.
- Humidity.
- Temperature.
- Radiation.
- Flooding.

For moderate energy pipework:

- Flooding.
- Radiation.

Note: Pipework failure assumptions for the PCC-3 and PCC-4 analyses are defined in Chapter 14.

<u>Jet impingement forces and pipe whip forces</u>

The consequences of jet impingement forces and pipe whip which may have an impact on system safety classified pipework, mechanical, electrical and instrumentation and control components are considered during the design stage. The resulting loads on building structures are also taken into consideration.

<u>Reaction forces</u>

Reaction forces are the forces caused by the fluid escaping via the leak and / or caused by the fluid pressure at the break and acting on the break cross section. Reaction forces are taken into consideration for the design of safety classified equipment, equipment supports, support anchors and the associated building structures.

Pressure wave forces, flow forces

Safety classified components and their internal equipment (e.g. reactor pressure vessel internals, steam generator tubes) located in the systems considered are designed to withstand flow forces resulting from postulated leaks and breaks. In the case of transient blowdown conditions, pressure wave forces including possible water hammer are considered as well.

Pressure wave forces (de-pressurisation wave forces) are forces which act on pipework sections between two bends and which occur from the blow down compression wave transferred through the fluid from the break.

Differential pressure forces, pressure accumulation

In the event of a postulated leak or break in a high energy line with a temperature ≥ 100°C, the mass and energy are released into the building. After leaving the break compartment, the fluid is dispersed to other connected sub-compartments. Differential pressures occur due to the flow restrictions causing additional loads on the structures in the safety classified buildings. Also, pressure build-up is taken into consideration for safety classified buildings (e.g. containment) with the exception of the nuclear auxiliary building (see Chapter 3).

The pressure increase in the sub-compartment is also taken into consideration in the design of the safety classified electrical and instrumentation and control system components.

Humidity, temperature, radiation

Safety classified electrical and instrumentation and control system components are designed to withstand temperature, humidity and radiation in the event of postulated leaks and breaks in the pipework. Humidity and temperature are only considered for pipework with a temperature ≥ 100°C. This is considered during the design of the areas which are subject to such loads.

Flooding

Safety classified mechanical, electrical and instrumentation and control components which must remain intact during a postulated leak or break are located above the maximum expected flood level.

The flood level is also considered during the design of the building structure.

2.2.4.1. Design principles for components used for reducing pipe breaks impact

Two types of restraints are provided where necessary to mitigate the consequences of pipe breaks:

- Large gap restraints. Restraints with large gaps are used when the rupture may be associated with a large deflection of the pipe.

- Restricted gap restraints. Restricted gap restraints are installed where major pipework movements permitted by large gap restraints cannot be tolerated. The purpose of the restricted gap restraints is to limit pipework deflection, for pipework subject to jet impact loads (gap restraints) and to prevent collapse in the event of a postulated pipework break (multiple path restraints).

Each type of restraint is designed in the following manner:

- Large gap restraints.

The flexible restraints, that is, those with a U bar, are designed to operate in the elasto-plastic range. The fastenings, such as the saddle, clevis pin, support bracket, the welded assemblies or anchor bolts are designed to operate in the elastic region.

The maximum deformation of the U bar is limited to an acceptable value which is verified by an analytical method. Pipe whip restraints are designed for single use, for a constant blow down force or an actual event. The minimum gap between the restraints and the pipework surface includes the thermal displacements and insulation thickness.

- Restricted gap and multiple path restraints

These restraints are designed for protection against pipe whip, using a load factor method static analysis. The force on the restraint is considered to be equal to the jet thrust load, multiplied by a dynamic load factor. A conservative dynamic load factor of 2 has been assumed.

2.2.4.2. Calculation techniques

The analysis of high energy line breaks may be performed in accordance with a modified dynamic method (pipe whip analysis) or by a simplified procedure, in order to verify the integrity of the main restraint components and the main civil structures, and to prevent secondary breaks resulting from failed pipework after the initial pipe break. The different acceptable methods for such an analytical approach for the assessment of pipework behaviour may be found in ANSI/ANS-58.2-1988.

The analytical design procedure for restraints is normally based on one of the following simplified methods:

Static analysis

The jet thrust force is represented by a conservatively amplified static load, and the restraint is analysed statically. The amplification factor used to determine the magnitude of the forcing function is based on the choice of a conservative value as obtained by comparing the factors derived from a detailed dynamic analysis performed on comparable systems.

Energy balance analysis

The kinetic energy generated during the first quarter circle movement of broken pipework imparted to the pipework and / or restraint system through the impact is converted into equivalent strain energy. The pipework and restraint deformations are compatible with the level of absorbed energy. A constant thrust is used in the energy balance analysis. It is taken as being equal to the initial pulse of the forcing function. However, a value below the initial pulse value may be used, if it is shown to be conservative in comparison to a standard dynamic analysis.

The thrust for each postulated pipe break is determined by a permanent load function. The thrust magnitude is:

$$T = K \cdot P \cdot A$$

Where:

T = thrust force.

P = system pressure prior to pipe break (operating pressure).

A = pipe break area.

K = thrust coefficient.

The value of K is one of the following:

K = 1.26 for saturated or superheated steam, water or steam/water mixture,

K = 2.0 for non flashing, sub-cooled water.

2.3. DESIGN VERIFICATION [REF-1] TO [REF-5]

2.3.1. Analysis of the local effects

2.3.1.1. General points

Sensitivity studies are performed for certain initiating events in order to show the absence of any cliff-edge effects in terms of radiological consequences.

The local effects are divided into compression wave forces and the effects on the systems caused by an increase in flow within the affected system and effects acting around the system:

- Compression wave forces and increased flow forces;
- Jet impact forces;
- Reaction forces;
- Pipe whip.

In addition, spray effects from failures in low energy systems are considered for electrical components and I&C components, where unacceptable consequences could occur. Protective measures for these components are provided in accordance with equipment qualification guidelines.

Compression wave forces and increased flow forces are only significant in case of sudden breaks or breaks of a large cross section, and are thus only analysed for such cases. This analysis must calculate the forces on the internal structures of components connected to the fluid system (e.g. forces on the reactor vessel internals in case of breaks in the pipework connected to the reactor coolant system). In addition, compression waves generate forces on the pipework supports which are considered in the context of the reaction force analysis.

Jet impingement forces must be considered, in case of breaks and leaks, with respect to the consequential effects on neighbouring systems, components and structures. The resulting loads must be taken into consideration by ensuring that the loads are covered by the design or by providing appropriate protection measures, e.g. restraints or additional supports.

Reaction forces due to leaks or breaks acting on the relevant pipework supports must be taken into consideration in the calculations required for these supports.

Pipe whip must be considered, in case of breaks with respect to possible impact on neighbouring systems, components and structures.

With respect to the consequences on other pipework, it is assumed for pipe whip that:

- Breaks may occur in target pipework with a diameter less than that of the whipping pipe;
- Consequential leaks may occur in pipework with a diameter greater than that of the whipping pipe providing the target pipe has a wall thickness below that of the whipping pipe

The assumptions for consequential failure are shown in Section 13.2.2 - Figure 1.

2.3.1.2. Buildings to be considered

The local effects of failures in high energy lines in the following safety classified buildings must be analysed:

- Reactor building;
- Safeguard buildings, including the main steam and feedwater valve compartments;
- Fuel building.

2.3.1.3. Installation requirements relative to the avoidance of inadmissible consequential effects

Protection requirements must be defined for defining maximum acceptable effects on adjacent systems, in case of failures of high energy pipework. These protection requirements are based on the following rules:

- In case of a loss of primary coolant accident (LOCA), the integrity of the containment including the pipework sections near the containment penetrations, as well as the operability of the containment isolation valves, must be ensured in order to prevent the release of radioactivity outside the containment;
- Systems required to shutdown the reactor, maintain sub-criticality, and remove residual heat, must not be adversely affected by a pipework failure;
- A consequential failure in the small diameter impulse lines and cables of safety classified components is admissible if the resulting actions are not detrimental to safety or if the components are fail safe. If this is not the case, detailed failure analyses must be performed;
- As a general rule, the same protection requirements must be applied to the safety classified supporting systems as are applied to the safety classified systems themselves.

The protection requirements are important in case of high energy line failures. In certain instances, exemption from these protection requirements is acceptable, where an appropriate justification is provided.

2.3.1.4. Integrity of radiological barriers

In case of pipework failure, the integrity of at least one of the following barriers is required:

- Reactor coolant pressure boundary, including the steam generator tubes;
- Containment.

Reactor Coolant Pressure Boundary (RCPB)

The reactor coolant system isolation valves must be located as close as possible[1] to the reactor coolant system.

In order to prevent a consequential LOCA in the case of a postulated break in pipework connected to the reactor coolant system, provision must be made for protection devices.

Protection of the RCPB is not the last line of defence and, as a result, this protection must be seen as a contribution to a defence in depth approach.

In case of failures in pipework not connected to the RCPB, e.g. failures in main steam lines or main feedwater lines, the isolation of the reactor coolant system must remain operable in order to ensure integrity of the RCPB.

Containment

When the containment function is required (release of reactor coolant inside the containment), integrity of the pipework sections between the containment penetration and the containment isolation valves must be ensured.

The containment isolation valves must remain operable following release of reactor coolant inside the containment.

For pipework which penetrates the containment, postulated failures between the isolation valve and the fixed points located beyond the valve require the protection of the:

- Containment;
- Pipework sections between the containment and the internal and external isolation valves, the fixed points beyond the isolation valves and the isolation valves themselves;
- Power supply and the signal connection to the isolation valve.

However, if the initiating failure occurs in the area between the isolation valves, or close to them, one of the isolations is lost. In this instance, the penetration itself performs the containment function, as well as the pipework section outside containment, which must remain intact and leak-tight, i.e. there is no propagation of damage through the containment penetration.

The containment isolation valves are located as close to the containment as possible.

An internal reactor building isolating component is added to the RIS [SIS] system injection lines, which is specific to the internal reactor building containment isolation.

---

[1] It is essential that there is a minimum distance in order to prevent potential damage resulting from the thermo-hydraulic stresses.

In order to avoid pressurisation in the annulus between inner and outer containment buildings, the containment penetrations for high energy pipework containing fluid with a temperature ≥100°C is fitted with protection devices (e.g. double sleeved or guard pipework).

2.3.1.5. Preclusion of breaks resulting from consequential damage

Due to application of the HIC claim, breaks are discounted in certain high energy systems (see sub-section 2.2.2.1.3).

Consequential damage to systems where the HIC claim applies must not occur due to other events.

2.3.1.6. Fulfilment of the required safety functions

In principle, the safety functions must be ensured using redundant means, segregated by divisional separation or by concrete structures for areas without divisions. Certain specific installation requirements are described below, in particular in terms of local effects due to internal hazards (e.g. pipe breaks):

- In order to comply with the single failure criterion for the required RIS [SIS] trains, the LOCA must be limited to one leg (hot or cold) of one reactor coolant system loop. In addition, the RIS [SIS] lines which do not inject into the break must remain intact;

- This also concerns consequential damage to the pressuriser spray lines (connected to the cold leg of loop 2 or 3). However, a break in a spray line may result in a simultaneous LOCA via the hot leg (connection of the pressuriser surge line) and the cold leg (connection of the spray line to loop 2 or 3). These cases are covered by the analyses of cold leg leaks and breaks;

- As a general rule, the pipework installation must be performed in a way which prevents consequential failures of the secondary system in case of a failure in the primary system and vice-versa;

- The isolating function of the secondary side must be ensured in a way which isolates the affected steam generator in case of failure in the main steam or feedwater system and all other secondary side leaks which cannot be isolated;

- Isolation of the affected pipework in case of a failure which can be isolated in the lines connected to the steam generators must be ensured (e.g. by fixed points which protect the isolation valves);

- A failure of secondary side pipework must not lead to simultaneous depressurisation of two steam generators, unless it is possible to demonstrate that this is acceptable from a safety perspective.

- Consequential failures between steam and feedwater lines of the same steam generator must be avoided.

- Unacceptable consequential failures of the EVU [CHRS] system must be ruled out by using suitable installation (layout) provisions.

- In case of pipework failures with consequential damage to other pipework, the total fluid loss must remain within the limits of the global effects analyses.

2.3.2. Analysis of overall consequences

2.3.2.1. Flooding

(See section 8 – Protection against internal flooding)

2.3.2.2. Harsh environmental conditions (increase in pressure, temperature, humidity, radiation and release of boric acid)

The qualification of the relevant electrical and I&C equipment must be performed such that the harsh environmental conditions resulting from the postulated failures can be supported even at the end of the unit service life (consideration of ageing).

2.3.2.3. Pressure, Temperature, Humidity

Failure of pipework carrying hot water ($T \geq 100^{\circ}C$) or steam must be analysed taking into consideration the environmental conditions in the safety classified buildings.

Representative cases must be determined for the safety classified buildings listed below. The systems and components required to achieve the safety objectives must be designed so that they remain operational in case of an event which causes these harsh environmental conditions. In particular, the divisional separation should not be compromised by the propagation of degraded ambient conditions, through the implementation of appropriate measures [Ref-1].

The following buildings must be analysed in relation to the effects of pressure, temperature and humidity:

- Reactor building;
- Safeguard buildings, including the main steam and feedwater valve compartments;
- Fuel building.

The systems and components of one division in the diesel generator buildings and the pumping station may be subject to failures caused by harsh environmental conditions, if the systems which cause these conditions are located in these buildings.

The propagation of the harsh environmental conditions from the non-safety classified buildings or from the nuclear auxiliary building towards the safety classified buildings must be prevented using appropriate measures.

2.3.2.4. Radiation, release of boric acid

The global effects caused by radiation and the release of boric acid must be assessed for the required systems and components. Qualification of these components against radiation and boric acid release is required inside the containment and is described in the RCC-E.

2.3.2.5. Differential pressure forces for the building structures

The forces caused by differential pressure must be taken into consideration.

SECTION 13.2.2 - TABLE 1

Failure assumptions for the systems in which the 2% criterion is applied

Systems	Failure assumptions Back up (low energy)	 Operation (low and high energy)
Back up system for accident control	Size of break equivalent to a DN 50 pipework breach treated as enveloping case	-
Classified systems used in normal operation in low and high energy modes	Size of break equivalent to a DN 50 pipework breach treated as enveloping case	Size of break equivalent to a DN 50 pipework breach treated as enveloping case

SECTION 13.2.2 - TABLE 2 (1/4)

Summary of failure assumption for the high energy pipework systems (lines with DN>50)

System	**Respective Line in System Section**	**RCC-M Classification**	**Failure assumptions Breaks**	**Leaks**	**Comments**
Primary system	Main reactor coolant pipework	C	-	Y	The local loads caused by leaks are practically negligible for the design; for additional assumptions (see Sub-chapter 5.2)
Main steam system	Main steam lines from the SG to the containment's fixed points	C	-	Y	The local loads caused by leaks are practically negligible for the design; for additional assumptions (see Sub-chapter 10.5)
	Main steam lines from the containment's fixed points to the fixed points downstream of the main steam isolation valves.	C	-	Y	The local loads caused by leaks are practically negligible for the design.
	Main steam lines downstream of the above mentioned section	NC	Y	Y	
	Main steam discharge lines downstream of the safety valves and the pressure reducing isolation valves	C	-	Y	Failure assumptions for the accident control backup systems
	Heating lines	C	Y	Y	
Water supply system	Water supply lines from the SG to the water supply isolation valves	C	Y	Y	

C = Classified / NC = Non-classified

SECTION 13.2.2 - TABLE 2 (2/4)

System	Respective Line in System Section	RCC-M Classification	Failure assumptions Breaks	Failure assumptions Leaks	Comments
Water supply system	Water supply, start-up and shutdown lines upstream of the water supply isolation valves	NC	Y	Y	
Pressuriser system	Expansion line	C	Y	Y	
	Pressuriser spray lines	C	Y	Y	
	Pressuriser discharge line	C	-	Y	Failure assumptions for the accident control backup systems
Safety injection / Cooling of the reactor at shutdown	Lines between the main primary pipework and the first isolation valve	C	Y	Y	
	Lines between the first isolation valve and the second isolation valve	C	Y	Y	
	Accumulator injection lines between the accumulator and the second isolation valve towards the main primary pipework	C	Y	Y	
	Other RIS [SIS] / RRA [RHRS] lines (beyond the second isolation valve towards the main primary pipework)	C	Y	Y	(section fulfilling the RRA [RHR] function in a closed system)

C = Classified / NC = Non-classified

SECTION 13.2.2 - TABLE 2 (3/4)

System	Respective Line in System Section	RCC-M Classification*	Failure assumptions Breaks	Failure assumptions Leaks	Comments
Chemical and volume control system with seal injection for the reactor coolant pumps	High energy pipework sections RCV [CVCS] charging lines towards the main primary coolant pipework, the pressuriser and the reactor coolant pumps Main reactor coolant system discharge pipework towards the HP reducing valve.	C	Y	Y	
	Other sections of pipework (low energy)	C	-	Y	Only relevant for flooding
Emergency feedwater system	SG lines towards the non-return valves	C	Y	Y	
	Lines between the non-return valves and the isolation valves	C	-	Y	Failure assumptions for the accident control backup systems
	Lines between the isolation valves and the emergency feedwater pumps	C	-	Y	Failure assumptions for the accident control backup systems
	Other lines between the emergency feedwater supply tanks and the pumps (low energy)	C	-	Y	Only relevant for flooding and the loss of pipework functionality

C = Classified / NC = Non-classified

SECTION 13.2.2 - TABLE 2 (4/4)

System	Respective Line in System Section	RCC-M Classification	Failure assumptions Breaks	Failure assumptions Leaks	Comments
Steam generator blow down system	Lines between the SG and two secondary side isolation valves	C	Y	Y	
	Lines downstream of the two secondary side isolation valves and the reducing tank	NC	Y	Y	
	Reducing tank	NC	Y	Y	The break is admissible because it is located in a separate compartment
	Lines in the containment from the reducing tank towards the water supply tank	NC	Y	Y	
	Containment isolation for the above mentioned line	C	Y	Y	
	Above mentioned line downstream of the external containment isolation valve	NC	Y	Y	
	Line from the reducing tank towards the heat exchanger	NC	Y	Y	
	Lines from the heat exchanger towards the containment isolation	NC	-	Y	Only relevant for flooding
	Containment isolation for the above mentioned line	C	-	Y	Only relevant for flooding
	Lines in backup building 4 and the nuclear auxiliary building	NC	-	Y	Only relevant for flooding in backup building 4. No analysis of the indirect failures in the nuclear auxiliary building, (See Chapter 3)

C = Classified / NC = Non-classified

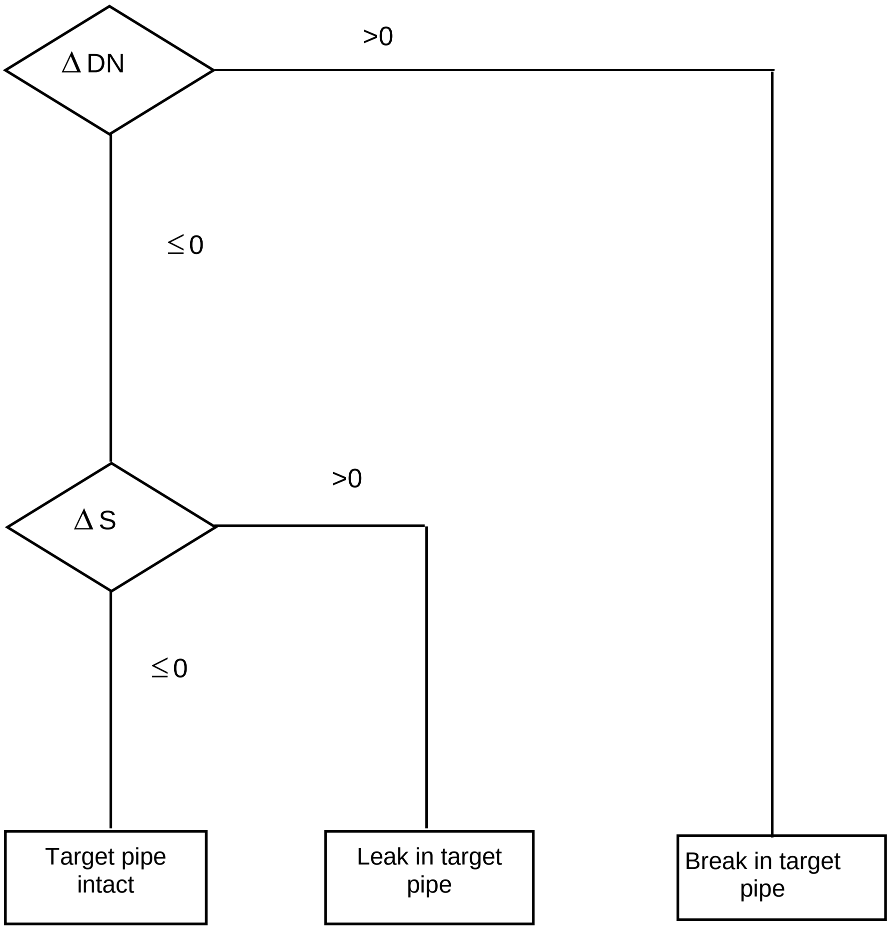
SECTION 13.2.2 - TABLE 3

Effects of pipework failure (summary)

Effects from	Effects on
Jet impact forces	Building structures, components
Pipe whip	Building structures, components
Reaction forces	Building structures, components
Compression wave forces	Components
Flow forces	Components
Differential pressure	Building structures
Pressure accumulation	Building structures, electrical and control system equipment
Humidity	Electrical and control system equipment
Temperature	Building structures, electrical and control system equipment, components
Radiation	Electrical and control system equipment
Flooding	Building structures, components

SECTION 13.2.2 - FIGURE 1

Postulated secondary failures caused by pipe whip



Δ DN. nominal diameter of the pipe subject to whip less the nominal diameter of the target pipe

Δ S thickness of the wall subject to pipe whip less the thickness of the wall in the target pipe

3. PROTECTION AGAINST FAILURES OF TANKS, PUMPS AND VALVES

3.1. SAFETY REQUIREMENTS AND DESIGN BASIS

3.1.1. Safety objectives

The general safety objectives for internal hazards are given in Sub-chapter 3.1

As for all other internal hazards, equipment required to perform the main safety functions must be protected against the unacceptable effects of failure of tanks, pumps and valves.

3.1.2. Requirements for protection against failures of tanks, pumps and valves

3.1.2.1. Identification of risks

The same effects as those considered in the case of pipework failures, except for the effect of pipe whip, must be considered in case of failure of tanks, pumps and valves.

The possibility of missile generation must also be considered, for failures in high energy tanks, pumps and valves which are not classified submitted to M1, M2 or M3 requirements (see Sub-chapter 3.2). The approach for protection against these projectiles is discussed in section 4.

3.2. DESIGN VERIFICATION

3.2.1. Classified equipment (M1 / M2 / M3 requirements)

Gross rapid failure of these components is not considered credible due to the material characteristics, the conservative design applied to each item of equipment, the manufacturing quality controls and the construction, operation, maintenance and inspection regimes.

For bolted devices, breaks are excluded due to the large number of bolts. It is assumed that the loss of one bolt will only result in leakage.

For the consequences of leaks from tanks, pumps and valves, it is considered that the postulated leak and break size (cross sectional area) in connected pipework, including associated welds, are bounded by the following effects:

- System analysis (e.g. over cooling transients, reactivity feedback, emergency core cooling, redundant design of the safety systems),
- Increased ambient conditions (e.g. pressure, temperature, humidity, radiation),
- Flooding of buildings,
- Forces acting on safety-related structures and components (jet impingement and reaction forces, pressure waves, flow forces and differential pressures).

However, even if the breaks are not considered credible, it is verified for defence in depth purposes, using realistic assumptions, that failure of these components would not lead to unacceptable consequences [Ref-1].

For those components 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 High Integrity Components (HIC) are listed in Sub-chapter 3.1 and presented 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.

3.2.2. Non-classified components

For components which are not required to comply with the quality M1, M2 or M3 requirements (see Sub-chapter 3.2), assessment of consequential failures due to breaks, is performed on a case by case basis.

The following criteria are considered:

Moderate energy components

For these types of component, an analysis must be performed for flooding, which is not restricted in terms of the size and the location of potential failures. If required, failure assumptions may be applied on the basis of an assessment of the quality assurance requirements applied to the component.

High energy components

As a general principle, the installation of non-classified high energy components in safety classified buildings (with the exception of the Nuclear Auxiliary Building), is kept to an absolute minimum.

For non-classified high energy components (not submitted to M1, M2 or M3 requirements), no restrictions are applied to failure assumptions, and all consequential effects must be considered.

4. PROTECTION AGAINST MISSILES

4.1. SAFETY REQUIREMENTS AND DESIGN BASIS

4.1.1. Selection and description of missiles

There are two general sources of postulated missiles:

a) Failure of rotating equipment;

b) Failure of pressurised components.

These missiles may cause damage to equipment or structures (see Sub-chapter 3.1).

<u>Missiles resulting from failure of rotating equipment</u>

Missiles could be generated by postulated failures in the following rotating components:

- Pumps,
- Fans,
- Compressors,
- Electric motors,
- Turbines.

With regard to postulated missiles from pumps, a distinction is made between centrifugal pumps and piston pumps.

For centrifugal pumps, the greatest amount of stored energy is the rotating energy. It is assumed that failures may result from failures of rotating parts or excessive stresses. However, this energy is not sufficient to generate missiles which could cause unacceptable damage. For pump impellers in particular, pump manufacturer's experience has shown that a missile generated by an impeller does not penetrate the pump casing.

This principle also applies to piston pumps, as they have a low level of transfer energy, as well as to fans, electric motors and compressors.

The same principle applies to missiles originating from electric motors, as their stator acts as a protective case against any potential missiles.

The generation of missiles from the turbine located in the turbine hall and the reactor coolant pump flywheel is taken into account.

<u>Missiles from failure of high energy components</u>

The potential for components to become missiles is analysed if they meet the criteria for high energy components.

Breaks in safety classified components (see RCC-M - Sub-chapter 3.8) (vessels, tanks, pumps and valves) are discounted: consequently no missiles are postulated for this class of component. This also applies to welded flanges, (e.g. for temperature sensors). However, for defence in depth purposes, it is verified, using realistic assumptions, that failure of these components with missile generation would not lead to unacceptable consequences. Components for which this demonstration cannot be achieved are classified High Integrity Components [Ref-1].

The installation of non-classified high energy components in safety classified buildings is limited where reasonably practicable. When this is not possible, the potential for missile ejection must be assessed.

In the case of pipework breaks, the generation of missiles is not considered due to the type of materials used and based on experience; however, effects due to pipe whip are analysed (see section 2 of this sub-chapter).

Missiles resulting from ejection of the pressuriser heaters, or rod cluster control assembly, are discounted on technical grounds, as their pressure retaining parts form part of the reactor coolant system pressure boundary (RCC-M level 1). The ejection of control rods is considered as a limiting accident (PCC-4).

A detailed study of nuts, screws and bolts as potential missiles is not considered necessary due to the low level of stored elastic energy.

Due to the specific nature of their construction and high penetration capability, the ejection of rod cluster control assemblies (considered locally inside containment) and valve parts (e.g. valve stems) must be assessed within the scope of pressurised equipment failures.

4.1.2. Protective measures taken against missiles

In the nuclear power plant design stage, provision is made for risks due to the missiles generated inside containment or other structures, in rooms outside of the containment containing safety equipment, and missiles generated outside the buildings but inside the site.

Due to their importance to plant safety, missile protection measures are taken for the following buildings:

- Reactor building, including the internal structures,
- Safeguard buildings,
- Fuel building,
- Diesel generator buildings,
- Pumping station.

The approach applied for protection against internally generated missiles is spatial separation of the different F1 system trains into different building divisions. This includes the associated auxiliary systems and the power and fluid supply systems. The divisions are structurally separated by partition walls.

In addition to the partition walls between the divisions, further concrete structures are provided around individual redundant equipment items (e.g. partition walls between the different reactor coolant system loops in the containment, missile protection zones in the containment where appropriate, and separation of individual components) thus providing additional shielding.

These concrete barriers prevent internally generated missiles from penetrating into other divisions. Damage within one division is permitted from a safety perspective.

In addition to the measures taken inside the containment to prevent the effects of missiles on other redundant equipment, it must be ensured that the equipment inside the containment which contains radiological material, and the containment itself, are not damaged simultaneously by a missile. This is achieved primarily by the partition walls provided between the individual reactor coolant system loops, or by the arrangement of the reactor coolant system within the missile protection zone or specific valve and steam generator compartments.

Based on the concept of defence in depth, the mechanical and structural measures described above ensure overall protection against missiles. In addition, the probability of internally generated missiles is reduced by the consistent application of safety oriented design and engineering principles. For example, the use of preventive measures such as over-speed trip protection devices, equipment restraints and valve stem threads which securely retain the valve in the event of mechanical failure.

In addition, the high level of quality assurance applied during the design, manufacture, installation, inspection pre-service and in-service in accordance with the relevant codes and standards, and the regular maintenance regime, ensures that the probability of missile generation will be extremely low.

The multiple measures described above ensure that the generation of missiles and the unacceptable consequences of missile effects, given the probability of generation, impact and possible damage, are so improbable that further detailed analyses are not necessary. Whilst it is not considered necessary to perform an analysis of each individual missile source, worst case scenario analyses is performed considering certain representative internal missiles.

Safety classified buildings are analysed to demonstrate that the thickness of the missile resistant barriers are adequate. In order to demonstrate that the thicknesses of the barriers are adequate for the worst case scenario, various representative missiles are analysed.

Whilst a systematic functional analysis is not performed for missile protection, it is confirmed that the design features (e.g. thicknesses of walls, raft foundations) are sufficient to protect against representative missiles considered.

4.1.3. Missile protection during shutdown conditions

The above argument also applies to unit shutdown conditions. The confirmation of the design (e.g. thickness of walls, raft foundations) is also applicable to shutdown conditions, given that missile barriers are normally available.

Attention is given to potentially dangerous missile sources which are temporarily introduced to the unit during the shutdown conditions.

4.1.4. Barrier design procedure

Missile protection barriers and structures are designed to protect plant against a missile impact, and to prevent damage to structures, systems and components requiring protection.

The calculation methods used for design of missile resistant barriers and structures are given in ETC-C (see Sub-chapter 3.8).

The acceptance criterion for the missile barriers is defined as:

- wall thickness > penetration depth.

Note: in addition to the penetration depth considered for missiles, protection barriers are also assessed against other design requirements, e.g. radiation protection, integrity in the event of pipe whip.

4.2. DESIGN VERIFICATION [REF-1]

4.2.1. Introduction

The missile safety analysis is the deterministic demonstration that the unit has acceptable protection against such a risk.

Missile protection must be considered for buildings which house and support mechanical equipment or I&C equipment with a F1 function.

In addition, the probability of internally generated missiles is reduced by the consistent application of safety oriented design and engineering principles.

It is only considered necessary to perform analyses of the worst case scenario for certain representative internal missiles.

Consequently, a systematic functional operational analysis is not performed for missile protection, but it is verified that the design features (thickness of walls and foundation raft/slab) are of sufficient integrity to protect against the chosen representative missiles.

For the UK EPR, it is intended that the alignment of buildings will ensure that structures, systems and components relevant to nuclear safety will be located outside the region vulnerable to missiles produced by turbine disintegration. The turbo-alternator unit design will also ensure a very low probability of energetic missiles being produced by turbine disintegration.

4.2.2. Analysis for the reactor building

4.2.2.1. Missiles generated inside the reactor building considered in the analysis

4.2.2.1.1. Reactor vessel, steam generators, pressuriser, accumulators, reactor coolant pump body and other high energy tanks

A failure within the reactor vessel, steam generators, pressuriser, accumulators, reactor coolant system primary circuit, pump casings and other high energy tanks, with sufficiently high classification (at least M3 requirements, see Sub-chapter 3.2), leading to the generation of missiles, is considered to be sufficiently unlikely for this mode of missile generation to be discounted. A massive and rapid failure of these components is not considered credible due to the material characteristics, the conservative design applied to each item of equipment, the manufacturing quality controls and the construction, operation, maintenance and inspections regimes.

However, for these components, in accordance with the concept of defence in depth, an analysis of the failures involving generation of missiles is performed [Ref-1], [Ref-2]. The components which could lead to unacceptable radiological releases are identified and then classified as "High Integrity Components" and are subject to appropriate requirements. Even if the failure of a main reactor coolant system loop is considered incredible, the loops are designed so that a break in one loop could not lead to failures in the other loops.

4.2.2.1.2. Valves

The following "valve" missiles, with different masses, are analysed in order to bound the characteristic range of missiles, based on the analysis of the worst case scenario, even if these missiles do not need to be postulated for the stated limiting conditions:

- Failure of a reactor coolant system safety valve mounted on top of the pressuriser, or failure of the additional valves provided for use in the case of a severe accidents. The three reactor coolant system safety valves are of identical design and are mounted on top of the pressuriser, in the same valve compartment.

- Failure of a chemical and volume control system RCV [CVCS] isolation valve. The isolation valves are located in a dedicated compartment and are separated from the containment by a concrete wall.

- Failure of a valve in the safety injection/residual heat removal system RIS [SIS] / RRA [RHRS]. There are four nearly identical, physically separate compartments, for the safety injection/residual heat removal system RIS [SIS] / RRA [RHRS], assigned to the four reactor coolant system loops. The analysis of missile effects is performed for failure of the largest diameter valve.

Based on the following arguments, the missiles analysed are considered representative of those from failures to other valves (including valves in other buildings):

- Similar valves designs enable similar failure assumptions to be used.

- The range of valve sizes (nominal bores) considered in the analysis, enable the masses of missiles analysed to be considered as representative.

- Failure considerations for high pressure valves bound the failure consequences of low pressure valves.

4.2.2.1.3. Control Rod Drive Mechanisms (CRDMs)

The failure of a Control Rod Drive Mechanism (CRDM) housing, which could cause the ejection of the Rod Cluster Control Assembly (RCCA), is not considered credible due to the material properties of the housing and the quality, construction and pressure testing of the CRDM housing.

However, it is postulated that the top cap on the CRDM could become loose and be accelerated upwards by the water jet. The following sequence of events is assumed to occur.

The RCCA and the drive rod assembly would be ejected from the core by a differential pressure of approximately 155 bar. The CRDM is assumed to be fully inserted at the beginning of the accident. The lower conical section of the drive rod will hit the collar of the Latch Unit and be stopped. The leakage path is minimised due to the strong contact between drive rod and collar. The kinetic energy is transferred from the mobile set via Latch Unit collar and CRDM flange connection to the RPV head adapter. The drive rod will stick inside the pressure housing and will not become a missile. The top cap with connected displacement limiter will be ejected together with the ejection locking cross (part of the vessel head equipment) and will be stopped by the pool slabs, which can withstand these loads. The top cap with connected displacement limiter and the ejection locking cross will fall onto the cable bridge, which is capable of supporting the respective loads. The CRDMs beneath the cable bridge would not be affected.

The rod ejection accident is analysed in section 5 of Sub-chapter 14.5.

4.2.2.1.4. Reactor coolant pump flywheel

A failure of the reactor coolant pump flywheel resulting in the generation of internal missiles could result in significant damage to surrounding components and structures. Therefore, special requirements have been defined to discount the risk of missiles generated by the reactor coolant pump flywheel. This component is classified as a High Integrity Component (HIC) [Ref-1] and must fulfil the strict requirements covering the material, design, manufacture and inspection. These requirements can be expressed in terms of five levels of prevention of gross failure:

a) Use of adequate material: high strength steel. The material chosen for the flywheel construction (20NCD14-07, technical specification M2321 of RCCM) is a high toughness material (K1C = 200 MPa m). This material can withstand high stress intensity factors

b) Design of the flywheel. The EPR Reactor Coolant Pump flywheel is composed of two disks, in order to limit the size of the potential loose parts in the event of flywheel failure. This design is justified in the design report [Ref-2], which analyses the following failure modes:

   - ductile failure
   - brittle failure
   - crack depth propagation (performed for the most adverse location, in the keyway)

   These analyses demonstrate the flywheel integrity under conditions of excess speed in the presence of defects

c) Pre-service inspections, using stringent acceptance criteria. Ultrasound inspection over 100% of the volume and surface inspections using dye penetrant or magnetic particle inspection are carried out during the manufacturing of the flywheel disks (both before and after final machining).

d) Pre-service tests. In factory overspeed tests are performed on each motor equipped with its flywheel, at 1.25 times the normal speed, which encompasses the maximum accidental overspeed of the pump rotor.

e) Monitoring during operation. Volumetric controls of the most highly stressed areas of the flywheel are carried out during the in-service inspections. For this purpose, the flywheel is designed with six axial holes allowing ultrasonic examination of the keyways corners. These inspections enable the monitoring of crack initiation and propagation, however unlikely.

The maximum break size of pipework which is connected to the reactor coolant system does not result in flywheel over-speeds able to lead to a loss of integrity.

4.2.2.2. Protection against internally generated missiles

Protection against missiles is provided by one or more of the following methods:

- Enclosure in compartments, i.e. the missile sources requiring protection are enclosed in compartments which walls prevent missile penetration;
- Use of barriers;
- Separation of redundant systems;
- Use of distance (location beyond the range of potential missiles);
- Use of restraints;
- Orientation and design of components.

4.2.2.2.1. Barriers around the reactor coolant system loops

The reactor coolant system pressure boundary up to and including the second isolation valve, is located in a missile protection zone or in specific valve compartments. This ensures that damage to the containment from missiles is not credible. This approach also ensures that missiles cannot damage the primary radiological barrier (reactor coolant system pressure boundary) and the secondary radiological barrier (the containment), at the same time [Ref-1].

The four reactor coolant system loops (with the exception of the crossover legs, where no missile potential risk exists) and the lower sections of the steam generators are physically separated by concrete structures.

4.2.2.2.2. Barriers around the pressuriser safety valves

The pressuriser relief valves are enclosed in a reinforced concrete structure containing the pressuriser, to ensure adequate protection against missiles [Ref-1].

4.2.2.2.3. Barriers above the Control Rod Drive Mechanisms (CRDMs)

Reinforced concrete slabs are installed above the reactor pressure vessel [Ref-1].

4.2.2.2.4. Arrangement of containment isolation valves

In order to reduce the probability of the loss of containment pressure boundary function due to internal missiles, the containment isolation valves are located as close as reasonably possible to the containment. As a result, the risk of damage to long sections of pipework due to missiles from neighbouring systems is largely eliminated.

To demonstrate the adequacy of the missile protection measures, calculations of the local consequences on the building structures (walls, slabs and foundation rafts), for certain representative missiles, are performed on a worst case basis [Ref-1].

4.2.2.3. Missiles generated outside the reactor building

For systems located in the reactor building, protection is provided by the reactor building itself, ensuring that a missile generated in another building cannot cause unacceptable consequences to a system located in the reactor building, (for aircraft crash see section 3 of Sub-chapter 13.1).

4.2.3. Analysis for the safeguard buildings

4.2.3.1. Missiles generated outside of the safeguard buildings

For buildings protected against an aircraft crash (see section 3 of Sub-chapter 13.1), protection is provided by the building structure and wall thickness. This prevents a missile generated from other buildings from having unacceptable consequences on the systems which are housed in these buildings.

For other components, including the main steam and feed water isolation valve compartments (2 by 2 arrangement), aircraft crash protection and therefore missile protection (see section 3 of Sub-chapter 13.1) is achieved by geographical separation.

4.2.3.2. Missiles generated inside the safeguard buildings

4.2.3.2.1. Mechanical zones of the safeguard buildings

The auxiliary safeguard buildings house the following safety classified systems:

- RIS [SIS] /RRA [RHRS],
- RRI [CCWS],
- SEC [ESWS],
- ASG [EFWS],
- Equipment for instrumentation and control and electrical systems,
- Essential heating, ventilation and air conditioning.

In addition, the two EVU [CHRS] trains are located in divisions 1 and 4, the third PTR [FPCS] train is located in division 1 and the MCR is located in the electrical section of divisions 2 and 3.

In accordance with the redundancies within the RIS [SIS] / RRA [RHRS], RRI [CCWS], SEC [ESWS] and ASG [EFWS], the mechanical section of the safeguard buildings forms four separate divisions. In addition to this divisional separation, the radiological controlled areas are separated by structural barriers. Further structural barriers are provided for the radiological protection of personnel.

As a general rule, components located in the safeguard buildings are installed in individual compartments or separated from adjacent components by walls. In general, valves are installed in separate valve compartments.

The valves located in the safeguard buildings are subject to pressures lower than those used as the basis for analysis in section 4.2.2.2 above.

Since missiles are not postulated, and divisional separation has been applied to the safeguard buildings, a specific missile protection analysis is not considered necessary for the mechanical zones of the safeguard buildings.

4.2.3.2.2. Electrical zones of the safeguard buildings

No pressurised systems are installed in the electrical zones of the safeguard buildings.

In addition, partition walls separate the redundant trains of equipment. The thickness of the partition walls are at least 300 mm.

A specific missile protection analysis is not considered necessary for the electrical zones of the auxiliary safeguard buildings.

4.2.3.2.3. Main steam and feed water valve compartments

The main steam and feedwater valve compartments are divided into four geographically / physically separated compartments. Given their geographical separation, the protection of the compartments by structural measures and the reactor building concrete shell, the possibility that a missile will affect all redundant trains is discounted.

Valves belonging to the VVP [MSSS] / VDA [MSRT] and ARE [MFWS] are located in separate compartments. Therefore the possibility that an internal missile caused by failure of the ARE [MFWS] impacting on VVP [MSSS} / VDA [MSRT] sections is discounted.

A specific missile protection analysis is not considered necessary for the main steam and feedwater valve compartments.

For the Safeguard Buildings, the only inspection requirement is to confirm adequate thickness of the structures to withstand impact of representative missiles [Ref-1].

4.2.4. Analysis for the fuel building

4.2.4.1. Missiles generated outside the fuel building

For buildings protected against an aircraft crash, protection is provided by the building structure and wall thickness. This protection prevents a missile generated from other buildings from having unacceptable consequences on the systems which are housed in the fuel building.

4.2.4.2. Missiles generated inside the fuel building

In the lower section of the fuel building, the two RBS [EBS] trains are segregated to prevent the loss of both trains due to missile impact. The structural separation is such that an internal hazard can only affect one of the two redundant main PTR [FPCS] trains and the associated intermediate cooling systems RRI [CCWS]. For the third PTR [FPCS] train, protection measures are designed to avoid any possibility of losing this train at the same time as the other two trains as a result of missile impact. Additionally, this train is cooled by an independent intermediate cooling system, located in safeguard building division 1. Therefore, consequential damage resulting from missiles would be limited to one redundant system, which as a general rule is acceptable.

For the upper level in the fuel building (level +0.00 m and above), the PTR [FPCS] redundant trains are located or protected so that only one redundant train is at risk from missiles. The fuel building structure protects the fuel pool itself.

The only inspection requirement is to confirm adequate thickness of the structures to withstand impact of representative missiles [Ref-1]

4.2.5. Analysis for diesel generator buildings

4.2.5.1. Missiles generated outside of the diesel generator buildings

Diesel generator buildings 1/2 and 3/4 (placed 2 by 2) are protected against an aircraft crash by geographical separation.

4.2.5.2. Missiles generated inside of the diesel generator buildings

The possibility of a missile affecting more than one train is prevented by partitions separating the trains.

All of the diesel motors have speed restriction devices. The diesel generators are used as safety systems and are not used during unit operation.

Therefore, a specific analysis is not required for the diesel generator buildings.

For the diesel generator buildings, the only inspection requirement is to check for adequate thickness of the structures to withstand impact of representative missiles.

SECTION 13.2.4 – TABLE 1

Missiles considered in the analysis

MISSILES	MISSILE LOAD RESISTANT BARRIERS
RCCAs	a) Concrete slabs covering the reactor pool
Valve sections (e.g. valve stems) acting as a representative missile	a) Walls, floors, ceilings surrounding the reactor coolant loops, as well as the pressuriser and the pressuriser relief valve room b) Missile protection zone (cylinder) c) Division separation structures, separation walls for the primary/secondary loops (reactor building, fuel building, safeguard building, raw water pumps building(s), diesel generator buildings) d) Structures between the main water supply valves station and the main steam valves station in the same loop and between different loops e) Fuel pool structure

5. PROTECTION AGAINST DROPPED LOADS

5.1. SAFETY REQUIREMENTS

A dropped load occurs if, during manoeuvre, the lifting device can no longer control the load on the hook.

A dropped load may lead to mechanical damage to the equipment or structures located near the lifting area. This is dependent on the weight of the load and the resistance of the impacted equipment or structure.

The impact may also cause the load to be damaged and this event must be taken into consideration, particularly if the load contains radioactive substances (e.g. fuel assemblies).

5.1.1. Deterministic approach

The approach for protection against dropped load is essentially deterministic.

According to this deterministic approach:

- A dropped load is postulated from any lifting device which does not have sufficient classification (see section 5.2.2 below) but only for one item of equipment at a time.
- The dropped load occurs during plant normal operating conditions (power operation or shutdown conditions).

5.1.2. Applicable regulations

The main regulations applicable to control lifting operations and equipment in the UK EPR are as follows:

- The Lifting Operations and Lifting Equipment Regulations 1998 LOLER. Statutory Instruments 1998 No. 2307
- The Provision and Use of Work Equipment Regulations 1998 PUWER. Statutory Instrument 1998 No. 2306
- The Management of Health and Safety at Work Regulations 1999
- The Supply of Machinery (Safety) Regulations 1992. Statutory Instrument 1992 No. 3073.

The above legislation mainly addresses the significant physical hazards that can arise from lifting operations and equipment.

5.2. DESIGN BASIS

5.2.1. Introduction

Protection against dropped loads is based on the following measures:

- Classification of the lifting devices and associated requirements,
- Installation or design rules for potential targets,
- Operational rules for lifting devices.

5.2.2. Classification of lifting devices

Lifting devices are classified in accordance with the results of a simplified hazard analysis. This analysis evaluates the consequences of a postulated dropped load from the associated lifting device.

The consequences are considered to be unacceptable, if they could lead to:

- A criticality accident or,
- A loss of decay heat removal function or,
- A release of radioactivity leading to radiation exposure in the vicinity of the unit which exceeds PCC-4 limits.

The associated lifting device is then classified as having “higher requirements”. These requirements enable the possibility of damage due to the dropped load to be discounted for design basis considerations.

The consequences are considered to be serious, if it could lead to:

- A non-isolable release of primary coolant into the containment or,
- A failure which leads to consequential failure of an F1 system or,
- A release of radioactivity leading to increased radiation levels inside the area which affects the classification of radiological zones.

The associated lifting device is then classified as having “additional requirements”.

Other lifting devices are not safety classified.

5.2.3. Installation rules

For lifting devices which are classified as having “higher requirements”, the lifting system and operations are designed such that the frequency of unacceptable consequences is adequately low.

The possibility of small loads being dropped (for example, valves, small motors) must be taken into account during the normal design of buildings (through consideration of maximum admissible temporary loads).

In order to minimise the effects from a dropped load, the design and layout of the site and its facilities are such that they:

- Minimise the direct effects of dropped loads on structures, systems or components;
- Minimise any interactions between a failed structure, system or component and other safety-related structures, systems or components;
- Ensure site personnel are physically protected from direct or indirect effects of incidents;
- Facilitate access for necessary recovery actions following an event.

Support facilities and services important to the safe operation of the reactor are designed and routed so that, in the event of incidents, sufficient capability to perform their emergency functions remains. Support facilities and services include access roads, water supplies, fire mains and site communications.

5.2.4. Operational rules

In addition to the measures applied to lifting devices to enable the probability of dropped loads occurring to be reduced or discounted, further measures are applied to minimise the risk. These measures are achieved by the application of administrative controls on the operation of the lifting devices in terms of:

- Restriction of operating periods,
- Limitation in lift heights,
- Use of prescribed routes for transporting heavy loads.

The following rules are applied in order to plan the load paths for heavy loads which are fixed to lifting devices [Ref-1]:

- Use of the shortest possible routes,
- Duration of the lifting operation to be optimised.

The load paths must be chosen so that:

- Stoppage times above critical locations (e.g. reactor pit) are as short as possible,
- The reactor pit should only be crossed during periods of approved maintenance.

In addition, unintentional travel above critical areas with heavy loads can be prevented by means of interlocks.

This approach is applied in all plant operational conditions, especially shutdown.

5.3. DESIGN VERIFICATION

The safety analysis of dropped loads is the deterministic demonstration that the unit has acceptable protection against such risks.

It must be demonstrated that:

- The classification is appropriate,
- The consequences of any postulated dropped load are acceptable.

5.3.1. Non-classified and Additional Requirements Equipment

For this kind of equipment, the demonstration is made following detailed studies, for each lifting device used in safety classified buildings in accordance with the dropped load methodologies [Ref-1] and [Ref-2].

This analysis must not take benefit from the application of operational rules described in section 5.2.4 above.

The assessment of dropped loads takes into account simultaneous effects, common cause failure, defence in depth and consequential effects. To achieve this, the analysis takes into account that:

- A hazard (i.e. dropped loads) may occur simultaneously with a facility fault, or when plant is unavailable due to maintenance;
- There is a significant potential for hazards to act as initiators of common cause failure, including loss of off-site power and other services;
- Dropped loads have the potential to threaten more than one level of defence in depth at once; and
- Dropped loads can arise as a consequence of events external to the site and should be included, therefore, in the relevant fault sequences.

Assessments are also made against the most onerous plant conditions. Sensitivity studies are also performed for certain initiating events in order to show the absence of any cliff-edge effects in terms of radiological consequences.

ALARP studies complete the studies for Additional Requirements lifting equipment [Ref-3] for some representative cases:

- Drop of a Fuel Assembly from the Refuelling Machine in the Reactor Building
- Drop of a Fuel Assembly from the Spent Fuel Mast Bridge in the Fuel Building (spent fuel pool and transfer facility)
- Drop of a 20 foot long and 20 ton container from the Set Down Area Crane

These additional assessments conclude that the consequences of a drop load were proven to be acceptable and that the design was assessed as ALARP in each case studied. Additional Human Factors studies (see Sub-chapter 18.1) concluded that the generic design includes suitable and diverse provisions to prevent significant direct human errors [Ref-4].

5.3.2. Higher Requirements Equipment

Although the failure of Higher Requirements lifting equipment is considered to be very unlikely, assessments for representative cases are performed [Ref-1] using a defence-in-depth approach with realistic assumptions:

- Drop of the Reactor Pressure Vessel (RPV) Closure Head on the RPV;
- Drop of a Reactor Cavity Cover Slab on the RPV Closure Head (plant state when the slabs above the reactor vessel are removed: State C);
- Drop of a Reactor Cavity Cover Slab on the Reactor Cavity Floor Slab (during State B);
- Drop of the Multi-Stud Tensioning Machine on the Reactor Cavity Floor Slab.

These additional assessments conclude that the consequences of a drop load were proven to be acceptable and that the design was assessed as ALARP in each case studied. Additional Human Factors studies (see Sub-chapter 18.1) concluded that the generic design includes suitable and diverse provisions to prevent significant direct human errors [Ref-2]. ..

6. PROTECTION AGAINST INTERNAL EXPLOSIONS [REF-1]

6.1. SAFETY REQUIREMENTS

The hazard considered is an event originating on the plant site with the potential to adversely affect or damage the equipment required for the three basic safety functions: Reactivity control, cooling of the fuel, containment of radioactive substances.

The general objective of the design provisions is to ensure that the safety functions of the systems and components, which are required to bring the plant in a safe shutdown state and to prevent and limit radioactive releases are not affected unacceptably.

The "defence-in-depth" principle has to be applied to the protection against internal hazards so as to limit the likelihood and the consequences of such hazards by the implementation of prevention, control and mitigation provisions.

In connection with the definition of the three basic safety functions consideration is given both to buildings containing systems necessary to reach and maintain a safe shutdown state, and buildings housing systems containing radioactive materials.

6.1.1. Consideration of combined events

The approach described here is applied under normal operating conditions.

In considering risk from internal explosions, potential dependencies are considered with the following hazards:

- earthquakes (including “earthquake events” which covers indirect impacts). This dependency is examined in particular for pipework at risk located in the nuclear island - with, as a requirement, the leak tightness of such pipework - and for process generated explosive gases. Potential loss of offsite power (LOOP) due to the earthquake hazard, is taken into account in the design.

- pipe whip effects following break of high energy pipes,

- fire potential of pipework carrying explosive gases or pressure tanks,

- risk of projectiles due to high winds,

- lightning.

No combination of an external or internal hazard or of an initiating event, with an independent internal explosion, is considered. In particular, two independent explosions are not considered.

6.1.2. Safety objectives

The requirements and combined hazards taken into consideration are reflected by the following safety objectives:

- An explosion should not adversely affect more than one element of a set of redundant F1 system;
- As far as reasonably practicable, an explosion should not trigger a PCC-3 or PCC-4 event;
- Furthermore, an explosion should not, in particular, adversely affect stability/integrity of :
    - safety classified buildings and fire safety barriers,
    - components whose failure is excluded by design, for example, pipework satisfying the HIC claim.

In all cases, a sufficient number of systems/redundancies enabling the plant to reach a safe state should maintain their operability. An explosion should not affect the habitability of the main control room.

In the event that the main control room cannot be accessed, the habitability of the remote shutdown station should be guaranteed. Furthermore, accessibility to perform local actions should be ensured, when necessary.

Finally, an explosion should not challenge safety objectives specific to other nuclear installations on the nuclear site.

The safety functions required to cope with the internal explosion hazard are classified F2.

6.1.3. Definition of requirements concerning internal explosion

6.1.3.1. Identification of risks

Internal explosions on the nuclear site may damage equipment or civil structures.

The potential sources of internal explosions may be found at three levels:

- Internal explosions within systems;
- Internal or external explosions of buildings which may be due to a release of explosive gases from systems, processes or tanks;
- Internal or external explosions of buildings which may be due to the failure of pressure tanks for gas or liquefied gas, explosive or not.

Explosions of electrical or mechanical equipment are assumed to be excluded (see section 6.1.3.2).

6.1.3.2. Approach for protection against internal explosions on a nuclear site

The approach for protection against explosions involves three stages:

- Prevention which consists of :
    - taking constructive or organisational measures to prevent and/or control all releases,
    - avoiding the formation of explosive atmospheres which may result from such releases,
    - avoiding the ignition of any explosive mixture formed,
    - preventing the risks in pressure tanks;
- Monitoring by providing detection systems, combined with preventive action;
- Limiting the consequences that consist in providing means for mitigating the effects of an explosion in respect to safety related targets. The possible presence of other nuclear installations on the unit has to be considered, when defining the potential targets.

6.1.3.2.1. Prevention

The main objective of the approach adopted is first and foremost to avoid the formation of explosive atmospheres. The following general approach is applied to prevention:

- As a priority, the sources of explosion must be eliminated. That is why, it is sought on the one hand, to eliminate removable features on the pipework at risk and, on the other hand, to avoid or "control" processes that generate explosive gases to limit their potential emission of explosive gases.
- The use of explosive gases or gas pressurised tanks is avoided wherever possible. Where it is impossible to eliminate such tanks, their presence is limited to the quantity absolutely necessary. This is also true in storage areas, whether temporary or permanent (e.g. gas storage yards).
- For rooms housing systems containing explosive gases, the basic objective is to avoid creating dangerous conditions. To meet this objective priority is given to eliminating potential sources of leaks, limiting removable features on systems, limiting releases and their concentration in the locations considered, in order to remove the main factors which could cause the formation of explosive atmospheres.

If these basic measures do not enable the risk of occurrence of dangerous explosive atmospheres to be reduced to a sufficiently low level, other protection measures must be applied. These measures should include consideration of measures available to avoid the ignition of explosive atmospheres.

For the risk of internal explosions in the systems, prevention is studied in terms of the design of the process and operating instructions.

Components are deemed not to be vulnerable to the stresses (mechanical, thermal, neutron, etc.) considered in the design.

The risks of explosions in mechanical or electrical equipment (motors, circuit-breakers etc) are generally excluded because of design provisions (use of dry transformers, circuit-breakers without oil tanks). If necessary, the risk must be considered and prevented by design, installation and operating procedures.

Furthermore, special attention based on administrative measures must be paid to additional potential sources of explosions (for example, compressed gas cylinders, paint, lacquers, and other chemicals) brought into the plant during plant outages or in preventive maintenance, for example (see section 6.2.4.4 “Temporary storage”).

6.1.3.2.2. Monitoring

Detection systems involved in the safety demonstration should be reliable. Preventive action should also be made clear to operators (alarm sheets available to the operator).

6.1.3.2.3. Limiting consequences

The consequences of an internal explosion in the unit must be analysed if the risk cannot be excluded in the design verification step. In this case, the risks of damaging safety targets should be assessed and, if necessary, eliminated. All equipment or parts of equipment, the loss of which would lead to challenge the safety objectives (see section 6.1.2) must be considered.

6.2. DESIGN BASIS

6.2.1. Rooms and locations at risk

In terms of the risk of explosions associated with gas inside and outside buildings, the regulations concerning the safety of the workers are applied.

Malevolent acts are outside the scope of the PCSR.

Rigorous management of stocks of flammable and explosive products on the site is assumed, including application of design limits (limits in quantities…).

A room or location is said to be at risk when it contains a system at risk with removable singular points (valves, man holes, non-welded connections), process generated explosive gas, or an explosive gas pressure tank.

It is considered that a system which carries an explosive gas is at risk when, under its maximum normal operating condition, the concentration of explosive gas is equal to or greater than the Lower Explosive Limit (LEL) of the gaseous mixture contained within the system. By conservative convention we use a LEL equal to the Lower Flammability Limit (LFL) (see section 6.3.2.1.3).

Liquids the flash point of which is less than 55°C, or for which the working temperature is greater than the flash point, are considered as explosive gases.

6.2.2. Gaseous systems at risk

Based on the general approach, given above, the following measures are in place to fulfil the design requirements for systems containing explosive gases:

- Prevention:
  - Implementation of provisions at the design stage which ensure that they are leak tight;
  - Design of rooms, equipment and ventilation, which do not lead to stagnation areas;
  - Taking the risks of shocks into account;
  - Electrical earthing of systems and equipment;
  - Marking of equipment in line with European Directive.
- The detection of explosive gases provided in rooms at risk in the buildings of the nuclear island and, outside, at least in those where an explosive atmosphere is likely to be formed on the basis of the assumptions adopted for the design verification.
- The implementation of suitably rated materials and devices (ATEX 2G or 3G) adapted to the gases concerned, if necessary and according to the characterisation of the rooms carried out at the design verification step.
- The checking and maintenance of systems.
- The air renewal rate (natural or mechanical) that should avoid the formation of explosive atmospheres, wherever possible.

6.2.3. Process generated explosive gas

Explosive gases generated by processes have to be avoided wherever possible. The quantities of explosive gases produced should be limited to what is absolutely necessary and their generation controlled to avoid creating an explosive atmosphere, including Loss Of Offsite Power (LOOP) situations following an earthquake.

The design requirements for processes which generate gases are based on the following aspects:

- Prevention:
  - the implementation of provisions to limit the generation of explosive gases, where technically possible, during the design phase,
  - the design of rooms, equipment and ventilation which should not cause stagnation areas,
  - the grounding and earthing of all systems and equipment,
  - Marking of equipment in line with European Directives.

  - o The detection of explosive gases provided in rooms at risk in the buildings of the nuclear island and, outside, at least in those where an explosive atmosphere is likely to be formed on the basis of the assumptions adopted for the design verification.

- The implementation of suitably rated materials and devices (2G or 3G) adapted to the gases concerned, if necessary and according to the characterisation of the rooms carried out at the design verification step.

- The air renewal rate (natural or mechanical), which should avoid the formation of explosive atmospheres.

6.2.4. Gas storage

The term storage refers to any area permanently housing the tanks containing gases, liquefied gases or liquid or flammable explosives, pressurised or liquefied gases, prior to use.

Note: tanks in use (connected) are considered to be an integral part of the systems.

6.2.4.1. Case of external storage areas (gas storage yards)

Risks associated with gas storage mainly concern external storage areas (gas storage yards) where significant quantities of gas are involved. A risk analysis approach based on taking the different hazards and potential safety targets into account has to be applied (see section 6.1). The design of storage areas shall be based on the safety demonstration, established on the basis of the prevention of the risks of explosion (see section 6.3.4.4) and the protection of safety targets with regards to potential explosions (see section 6.3.4.5).

6.2.4.2. Nuclear island buildings

Storage areas should be avoided within the nuclear island.

In situation where storage areas cannot be avoided, quantities must be limited and the hazard risks avoided, as follows:

- If such storage areas exist, the maximum quantity of explosive gas in a storage room must not exceed the equivalent content of a B50 / 200 bar cylinder (50 litres). The capacity of an individual tank must not exceed the size of a B20 cylinder. The storage area must be protected in terms of the hazards described in section 6.1.1 and the domino effects of an internal explosion, with the aim of demonstrating the absence of risk of spillage of the contents. As an additional precaution, it must be ensured that such storage areas are not created within fire safety sectors or in rooms at the interface between fire safety areas. Failure to comply with these rules should result in a specific safety analysis (based, for example on the principles adopted for gas storage yards).

- In the specific case of the fire extinguishers under continuous pressure, it should be ensured that they are not exposed to the effects of fire, which is generally the case, since these extinguishers are kept clear of combustion sources to remain accessible in the event of a fire.

6.2.4.3. Buildings outside the nuclear island

Outside the nuclear island and inside the buildings, the same approach as on the nuclear island is developed for limited storage areas. If larger storage areas cannot be avoided, they are dealt with in the same way as external storage areas (see section 6.3.3).

6.2.4.4. Temporary storage

Apart from the identified fixed gas storage yards, transient gas storage may be necessary during plant shutdown, preventive maintenance or other operations. These storage areas should be subject to appropriate risk analyses.

6.3. DESIGN VERIFICATION

The design verification for internal explosions in the nuclear power plant must demonstrate that the site has adequate protection against the explosion hazard.

This demonstration should be performed in accordance with the following principles:

- The rooms or locations at risk should undergo an analysis of the adequacy of the preventive measures in place,
- If the risk remains, an analysis should be performed on the consequences of an explosion against the safety targets located inside or outside the buildings.

6.3.1. Analysis rules

The initial conditions are those of normal operating condition (see section 6.1.1).

The single failure criterion and preventive maintenance are considered in the safety analysis of internal hazard scenarios.

Given their inherent characteristics, distinction has to be made between situations:

- Inside the nuclear island;
- Inside buildings within the site but outside the nuclear island;
- Outside buildings within the site outside the nuclear island.

6.3.2. Analysis of the risks of explosion in the Nuclear Island

6.3.2.1. Prevention of the risks of explosion

6.3.2.1.1. Release sources

These are assumed to be present in all rooms at risk.

6.3.2.1.2. Reference leak

In systems at risk, the reference leak fixed once and for all for the sizing and justification of the provisions taken is a break, the cross section of which corresponds to a guillotine break, whatever the diameter of the pipe concerned.

The concentrations and quantities of explosive gas, inside the systems concerned, are those equivalent to the maximum concentrations and maximum quantities present during normal operating conditions.

This leak is applied in each of the rooms at risk as defined in section 6.2.1, on the pipe that causes the bounding consequence in the concerned room.

For processes which generate gases the maximum flow rate of explosive gases under normal operating conditions is considered as well as the maximum quantity under normal operating conditions.

In the case of the storage of explosive gases, the reference leak corresponds to the guillotine break of the valve of the cylinder that causes the bounding risk in the room.

6.3.2.1.3. Lower Explosive Limit (LEL)

This limit varies depending on the gas concerned. We adopt standard conditions of atmospheric pressure, temperatures, and relative humidity.

For a mixture of air/hydrogen, the LEL is 18% in volume under the standard conditions of atmospheric pressure and gas mixture in air. (The upper limit is 74%). For hydrogen, due to the progressive nature of the ignition/explosion phenomenon, the LEL is taken equal to the LFL (Lower Flammability Limit) and is therefore assumed to be 4% under the same conditions. These limits must also be adapted in the case of a ternary mixture (using the Shapiro diagram) (e.g. air/nitrogen/H2).

6.3.2.1.4. Analysis of the adequacy of prevention and determination of rooms at risk

The assessment of rooms (or areas, if several rooms are linked via openings under normal operating conditions or if there is continuous air transfer) with potential risks is undertaken on the basis of the survey of rooms at risk (see section 6.2.1).

The flammable gas concentration calculations are performed based on the assumption that gas is homogeneous (in the case of hydrogen) in the local atmosphere or in the area analysed, and that at all points the gas concentration is equal to the average concentration. If the average concentration is less than or equal to the LEL the area is considered as non-hazardous.

If the average concentration is greater than the LEL, all possible parameters should be considered, to address the risk.

If it is not possible to obtain a concentration lower than the LEL, the room or the area is considered to be hazardous and sufficient provisions are made to eliminate the possible sources of ignition (limitation of electro-static charges, 3G category materials) throughout the source room (see section 6.3.2.2.4).

Thereafter, we refer to these rooms by the term "rooms at known risk".

The absence of ignition risk in an explosive atmosphere, ventilated by an air duct, should be verified up to the point of dilution, which enables the concentration of explosive gas to fall below the LEL. This check includes the ventilation ducts of battery rooms.

For process generated explosive gases (e.g. battery rooms), ventilation must be capable of resisting - in terms of functionality - the earthquake and backed-up in case of a LOOP situation due to the earthquake, in order to be considered as an adequate line of defence.

6.3.2.1.5. Risk of explosion inside systems [Ref-1]

With regard to the potential for explosion inside the systems, assurance will be given that the design provisions are able to remove this risk. For example, injection of chemical products will be performed using dedicated pipework in order to prevent any potentially explosive mixtures.

6.3.2.1.6. Risk of explosion of interconnected tanks

Tanks for non-flammable gases or liquefied gases under pressure connected to a system should be protected from the hazards considered in section 6.1.1 in terms of the risk of explosion. When the risk of domino effects due to fire exists, one of the possible protections may be to equip the tank with appropriate pressure relief valves (to prevent failure due to heating effects).

Tanks for gases, liquefied gases and flammable/explosive liquids connected to a system should be protected against the hazards defined in section 6.1.1. Accordingly, they have to remain leak tight in the event of an earthquake and not be exposed to the risk of domino effects due to fires.

Under such conditions, the explosion of interconnected tanks is not considered.

6.3.2.2. Analysis of the consequences of an explosion inside nuclear island buildings

As part of defence in depth, an analysis of the consequences of an explosion should be presented in each room or area where an explosive atmosphere is likely to be formed (rooms at known risk) [Ref-1]. The analysis consists in checking that the damage caused by an explosion does not affect the safety functions provided by the identified targets.

6.3.2.2.1. Identification of potential safety targets

Targets to be protected are all equipment, or parts of equipment, the loss of which would challenge the safety objectives defined in section 6.1.2.

6.3.2.2.2. Combined events considered

These are defined in section 6.1.1.

6.3.2.2.3. Study assumptions

In this case, specific terminology is used for the notions of source room, source area, buffer room, buffer area, adjacent room and protected room (see definitions below in section 6.3.2.2.4).

In particular, the following are considered as analysis assumptions:

- As an initial approach, that all equipment located in the source area are assumed to fail,

- All equipment located in a projectile's trajectory is assumed to fail,

- The pipework, heat exchangers, manual valves and electrical cables [Ref-1] located in the buffer rooms are intrinsically resistant to the effects of an explosion (unless they are in a projectile's trajectory): they remain undamaged. The following should therefore be taken into consideration among the potential safety targets in these buffer areas: equipment classified as safety equipment, such as tanks, pumps, motor-operated valves, electrical cubicles, sensors, limit switches (associated with classified equipment).

6.3.2.2.4. Source room hazard potential (common cause)

Source rooms are rooms identified at known risk.

The hazard potential of each source is assessed taking the following definitions and assumptions into consideration:

- The **source room** is the room where an explosive atmosphere is formed,

- The **source area** comprises the source room and rooms permanently and significantly (> 1 m^2) connected to them (vertically or horizontally),

- For a given source area, the successive **buffer rooms** are determined in terms of the main civil structures, the surface area of which is greater than 1 m^2, delimiting the source area or another buffer room, likely to act as a **pressure relief device** (doors, concrete blocks, shaft cover slabs, etc.), under the conditions described below. The group of buffer rooms is known as the **buffer area,**

- The civil elements with a surface area greater than 1 m^2 are also **potential projectiles** in the buffer area,

- Potential safety targets located in rooms separated from the source area by at least one buffer room, or a succession/combination of buffer rooms (that communicate with the source area following the pressure relief device actuation), the total volume of which is greater than that of the source area are assumed to be undamaged (**protected room**). In this conservative approach, we consider that the pressure relief devices disappear simultaneously or individually, in the source area or in a buffer room,

- Potential safety targets located in rooms separated from the source area by a buffer room or a succession/combination of buffer rooms (that communicate with the source area following the pressure relief device actuation), the total volume of which is less than that of the source area, are assumed to be undamaged unless they are located in the probable projectiles' trajectories generated by the explosion. This type of room is known as an **adjacent room,**

- In buffer rooms in direct contact with the source area, all equipment located in the potential projectile's trajectories at the interface with the source area is assumed to be destroyed. In the rest of the room the intrinsically resistant equipment is not affected,
- In the case of large source rooms, the room may act as a buffer area, subject to justification.

The walls/floors/ceilings delimiting the source areas have to be sufficiently resistant to explosion and maintain the functions assigned to them. If not, the impact on the level of safety should be acceptable (compliance with the safety requirements defined in section 6.1). In this approach, and if necessary and technically possible, components designed to reduce the effects of the explosion will be included.

6.3.2.2.5. Treatment of potential common cause failures

The analysis involving damaged areas and the safety target equipment results in a list of potential common cause failures.

For confirmed common causes, priority is given to a process, which aims to:

- Eliminate the risk by:
    - either eliminating the risk of explosive atmosphere,
    - or removing/protecting the safety targets.
- If not, reducing the risk:
    - by limiting the risk of ignition, by eliminating or moving potential sources of ignition or by installing ATEX 2G or 3G equipment throughout the source area.

6.3.3. Analysis of the risks of explosion inside buildings, outside the Nuclear Island

For each identified building, the risks of an explosion damaging safety targets will be assessed and, if necessary, eliminated.

6.3.3.1. Identification of potential safety targets

Targets to be protected are all equipment, or parts of equipment, the loss of which would challenge the safety objectives defined in section 6.1.

6.3.3.1.1. Combined events considered

These are defined in section 6.1.1.

6.3.3.2. Procedure

Reference leaks as defined for the buildings of the Nuclear Island are not considered. The possibility of damage to or failure of pipework or tanks is established by deterministic analysis (cause/effect) given the hazards considered.

For each room or part of a building, which is identified as at risk, an analysis is made of the possibility of eliminating the risk of explosive mixture formation. If this is not possible, the consequences on the safety targets are examined and sufficient measures implemented.

The treatment of a storage area shall be similar to that of the nuclear island (see section 6.3.2.1). In the event of exceeding the quantities accepted in the nuclear island, the approach recommended for gas storage yards will be adopted (see section 6.3.4).

6.3.3.3. Risk of explosion within systems

Design arrangements should avoid the risk of explosions within systems.

The prevention of the explosion of interconnected tanks shall follow the principles adopted for the nuclear island (see section 6.3.2.1.6).

6.3.4. Analysis of the risk due to explosions outside Nuclear Island buildings

6.3.4.1. Identification of potential safety targets

Targets to be protected are all equipment, or parts of equipment, the loss of which would challenge the safety objectives defined in section 6.1.2.

6.3.4.1.1. Combined events considered

These are defined in section 6.1.1.

For each gas storage yard, taking these events into account consists of checking the relevance of the assumptions and the corresponding limitation of hazard sources for the scenarios defined in section 6.3.4.6.

The possibility of damage to or failure of systems at risk (e.g. pipework) is established by deterministic analysis (cause/effect) of the events concerned.

6.3.4.2. Procedure

The risks of an explosion damaging safety targets should be assessed and, if necessary, eliminated, by prevention of the explosion or by the protection of safety targets.

- An identification of the installations at risk from an explosion, which could challenge safety, is performed on each site.

- With regard to the installations, an inventory is made of the equipment and products deemed to be at risk from an explosion including pressurised gas cylinders and their quantities, and the shortest distance between each source and target requiring protection.

- In addition, for the internal transport routes, an analysis is made of the number of vehicles passing which are likely to be a source of fire or explosion risk.

- The risks are analysed using typical bounding envelope scenarios based on the degradation modes of the following potential targets:
    - The thermal effects caused by an explosion,
    - The air pressure wave caused by an explosion,
    - The projectiles caused by an explosion.
- The different hazards sources for locations with a risk of explosion are studied:
    - The effects associated with the combined events considered in section 6.3.4.1.1,
    - The internal site road or rail traffic,
    - The consequential effect of fixed installations other than those at risk from an explosion, likely to be at the centre of a fire (spread of fire, thermal radiation),
    - The ignition of a gas leak and/or an explosion,
    - The risks associated with the maintenance/operation of gas storage yards.

6.3.4.3. Sources of risk

6.3.4.3.1. Main gases under pressure and flammable liquids found in a Nuclear Power Plant (NPP)

6.3.4.3.1.1. Mobile containers

The risks associated with the explosion of mobile containers (tanker trucks or gas cylinder delivery trucks, temporary work storage areas) are taken into account. The risks accepted should not challenge the assumptions and scenarios of the analysis carried out in this context.

It has to be verified that the provisions for transfer areas are adequate to prevent the possible fire of a delivery truck.

6.3.4.3.1.2. Tanks for liquefied gases

The BLEVES phenomena (Boiling Liquid Expanding Vapour Explosions) on liquefied gas pressure tanks are taken into consideration.

6.3.4.4. Hazards on locations at risk

6.3.4.4.1. Thermal hazard

No fixed or mobile (vehicle) source of fire which could give a thermal flux of more than 8 kW/m^2 on the target is allowed near a gas tank. The safety distances should be assessed on an individual basis. This may be subject to specific regulations.

The safety distances between the containers and any sources of fire will be determined by calculation, taking exposure times into account.

6.3.4.4.2. Explosion hazard

Given the regulation design requirements for pressurised tanks, the risk of a container being hit by a projectile following the failure of another similar container is discounted. The hazards due to failure of tanks of a different type are assessed on an individual basis.

Given the inherent and regulated design of pressurised tanks, it is considered that they are not vulnerable to overpressure failure.

6.3.4.4.3. Treatment specific to certain gases

The risk associated with heavy gases, such as Liquefied Petroleum Gas (LPG) or the presence of acetylene or other explosive gases, requires that these storage areas be separated by being placed in shielded compartments or placed at a sufficient distance so as to avoid any consequential effects.

The risk associated with hydrogen is related to its storage and the potential for a break (rupture) in the connecting pipe of the hydrogen cylinders. The consequences of such a leak may be discounted due to design provisions of the hydrogen storage including:

- Elimination of the consequences of an ignited jet by installation of blast walls and an exclusion perimeter between the hydrogen gas storage and the rest of the facility.
- Limitation of the consequences of a hydrogen explosion in a confined space by restriction of the number of hydrogen cylinders and installation of blast walls or deflectors.

6.3.4.5. Risks for safety targets

6.3.4.5.1. Thermal risk following an explosion or a fire

The threshold for domino effects is fixed at 8 kW/m^2. If justified different values are possible depending on the materials and structures concerned. The exposure duration must be considered in assessing the severity of consequences.

With regard to the increase in temperature caused by the fire, the deterministic approach takes account of the actual surface area of the fire pool, the possibility of its spreading towards the equipment to be protected, the decrease of the combustible mass, the height of the flames, the surface power densities and radiated power of the flames on each target to be protected.

6.3.4.5.2. Risk of overpressure following an explosion

With regard to the effect of the pressure wave, the resistance of the buildings housing the structures and equipment required to carry out the three basic safety functions defined in section 6.1, must be verified. It includes the verification of the building ventilation systems especially in terms of the risk of pressure wave penetration.

From a safety perspective, these buildings are designed to resist a steep-front triangular overpressure wave, attaining a maximum overpressure of 10 kPa and a duration of 300 ms.

6.3.4.5.3. Risk of projectiles following an explosion

With regard to the different projectiles resulting from a broken (ruptured) container, the integrity of the safety targets or the resistance of the buildings against projectiles must be verified.

With regard to the impact of missiles caused by an explosion the analysis may be probabilistic involving a single missile.

6.3.4.6. Procedure: scenarios chosen

Given the analysis undertaken on the identification of initiating factors for a container explosion, three bounding envelope scenarios (in term of consequences) are chosen:

- Risk of single explosion;
- Risk of internal consequential effects;
- Risk of explosions caused by a generalised fire of external origin.

The limiting criteria used for these scenarios are:

- The thermal flux: 8 kW/m^2 – with damage being dependent on the duration.
- The over-pressure wave: the assessment criteria are fixed at 10 kPa for the buildings.
- The projectile: 35 kg for B50 (50 litres) type cylinders. This projectile should be revised accordingly if gas containers other than B50 cylinders at 200 bar are used.

6.3.4.6.1. Risk of single explosion

A single failure or a hazard from an unspecified source (handling error, ignited jet, etc.), could cause the largest stored container to break (rupture) resulting in an over-pressure wave as well as a single projectile. There is no risk of a consequential effect on the neighbouring gas containers due to their intrinsic and regulated design.

This scenario is taken into consideration for transfer areas.

6.3.4.6.2. Risk of internal consequential effects

The leak of a container containing a heavy flammable gas may be the cause of a large-scale fire. Of the gases stored on the site, only the heavy flammable gases of the LPG type (butane, propane), acetylene or calibration gases can be the sources of such an internal fire, which could cause consequential effects.

The risks associated with the use of hydrogen on the gas storage yard should be also considered. These scenarios (a jet of flame or a Vapour Cloud Explosion (VCE)) may be the source of consequential effects. These risks exist around connected H_2 cylinders and their distribution system (supports and hoses), provided that the following scenarios are present:

- another gas pressure tank,
- any other obstacle.

The critical distances in relation with these components should be calculated.

The consequential effects caused by these scenarios may cause consequential but non-simultaneous over-pressure and multiple projectiles.

6.3.4.6.3. Risk of explosions caused by a generalised fire of external origin

In this third scenario, the containers explode under the effect of thermal radiation caused by a full fire outside the gas storage yard.

There are two major types of initiators, mobile sources, such as vehicles circulating inside the site, and fixed sources.

The main fixed hazardous sources close to gas inventories are the transformers. In this instance, the consequential effects caused by thermal radiation over all of the gas inventory installations must be considered, if a screen does not protect them.

The risk of a fire due to road or rail traffic on site is covered by the internal operating rules for gas storage.

6.3.5. Interaction with other nuclear installations on the nuclear site

The impact of the explosion scenarios on other nuclear installations on the site must be assessed, in terms of thermal effects, pressure waves, and projectiles, on the basis of the resistance thresholds specific to each.

Equally, account must be taken of the impact of the scenarios considered in the analysis of the risk of internal explosions on other NPPs on the site. It must be ensured that an explosion in a neighbouring NPP, which is deemed to be acceptable within the framework of the safety analysis specific to this nuclear site, will not have an unacceptable effect on the safety objectives for the EPR.

These aspects are outside the scope of GDA and will be addressed in site specific studies.

7. PROTECTION AGAINST FIRES [REF-1]

7.1. SAFETY REQUIREMENTS

The safety objective for fire protection is to ensure that the safety functions are performed in the event of a fire inside the installation, where the fire has the same characteristics as the reference fire.

This objective implies that:

- a fire must not cause the loss of more than one set of redundant equipment in an F1 system.
- the non-redundant systems and equipment, which perform the required safety functions must be protected against the effects of a fire in order to ensure continuous operation.
- a fire must not compromise the habitability of the control room. In the event that the control room cannot be accessed the accessibility and the habitability of the remote shutdown station must be assured.

7.1.1. Fire protection requirements

7.1.1.1. Postulated fire hazards

7.1.1.1.1. Internal fires

Fire is normally assumed to occur in any room which contains combustible materials and ignition sources. Coincidental occurrence of two or more fires, from independent causes, is not considered.

7.1.1.1.2. Consequential fires

Fires could also occur as a consequence of other internal or external hazards. In such cases the fire protection requirements include the following.

<u>Protection requirements for fire due to internal hazards</u>

PCC or RCC conditions that could lead to fire are LOCAs and severe accidents. This is due to the fact that during these events there is a potential release of hydrogen in the containment. The necessary measures for designing the containment as well as the equipment necessary to eliminate the potential ignition of H_2, or to control a hydrogen fire or explosion are described in the section on internal explosion hazards.

Protection requirements for fire due to external hazards

Earthquake

In the case of an earthquake, buildings designed to resist external hazards must not contain equipment, which is likely to release combustible materials or to create a source of ignition. An exception is made for the Nuclear Auxiliary Building and the Effluent Treatment Building where only the buildings themselves are seismically classified.

If the equipment inside a building is not designed to resist an earthquake, fire protection measures must be provided to resist the effects of these hazards.

All the fire protection components must comply with the criteria of the “earthquake event” analysis (see Sub-chapter 13.1 section 2.2). They also must not impair the performance of safety functions as a result of either their operation or failure.

Aircraft crash

The combination of an aircraft crash and an internal fire in a building is not applied when designing the fire protection systems. However, the distribution network protection system (geographical separation and structural protection) will ensure the availability of means of emergency fire fighting.

Extreme cold

The materials required for fire protection and concerning safety must be protected against conditions of extreme cold.

7.1.1.1.3. Combined hazards

Although there is no proven dependency, the following cases of combined events are taken into consideration for defence in depth protection.

PCC-2 to PCC-4 events

An independent fire is only assumed to occur during the post-accident phase and after a controlled condition has been reached following a PCC-2 to PCC-4 event. Nevertheless, the fire protection measures are available for the full duration of the post-accident phase.

N.B.: The possibility of a fire in the Main Control Room during the post-accident phase following a PCC-2 to PCC-4 event is discounted in the design. This is justified by the availability of sufficient fire protection measures and the presence of operating staff who would be able to rapidly extinguish the fire.

RRC events

RRC type events are very infrequent. As a result, the combination of an RRC event with an independent fire is assumed to occur only during the post-accident phase and no earlier than two weeks after the event.

Design-basis earthquake

An independent fire is assumed to occur only during the post-accident phase, and no earlier than two weeks after a design-basis earthquake.

The following protection concepts are applied:

- The detection and extinguishing systems within a fire compartment, in buildings where mechanical, electrical or instrumentation and control equipment necessary performing F1 functions are installed, must be seismic category 1 classified.
- It is assumed that repair or replacement measures can be made available, if required, within a two week deadline after the event occurrence.

External flooding

A combination of fire and external flooding is not considered. However, for defence-in-depth protection, the fire fighting system components at FA3 are designed to be protected against a 1000 year flood event (Maximum Design Flood Level (CMS)) and its consequences.

Fire during plant operation; shutdown conditions and maintenance phases

The fire protection concept described above must also be applied in shutdown conditions and maintenance phases.

The maintenance periods present a potential increase in the probability of occurrence of fires: however the presence of personnel will aid the rapid detection and extinguishing of fires, thus reducing the risk.

Specific administrative procedures (fire permits, increased monitoring etc) must be applied for any situation which deviates from the general fire protection concept.

Specific attention will be paid to the introduction of combustible materials and ignition sources (welding operations, paint, solvents, etc), as well as to possible degradations in the fire protection provision (loss of compartment integrity due to an open door, etc), during such periods. A fire safety analysis for each shutdown case must be provided.

7.1.1.2. Fire consequences

It is conservatively assumed that all equipment (apart from that protected by fire barrier devices or able to withstand the fire effects) present in the fire compartment where the fire is assumed to exist can no longer perform its normal function due to the fire.

A fire must not cause the loss of non-redundant safety equipment. Otherwise, this equipment must be protected or the potential for a fire must be eliminated.

A fire could lead to an additional PCC-2 event. In this instance, adequate system redundancies must remain available to control the event.

Where possible a fire must not lead to an additional PCC-3/PCC-4 event.

7.1.1.3. Management of potential heat loads

The possibilities of storing combustible materials for operational requirements in industrial buildings are assessed and taken into consideration at the design stage. In particular, measures are taken to ensure fire protection in the storage areas if necessary.

7.1.2. Principles of the fire protection approach

The main approach for protection against fire is deterministic. This approach is complemented by a probabilistic safety assessment (see Sub-chapter 15.2).

The principles are as follows:

- The fire is assumed to occur in any plant room, which contains combustible materials and an ignition source.
- Coincidental occurrence of two or more fires, from independent causes, affecting rooms in the same or different plant is not taken into consideration.
- The ignition of any combustible material present in buildings must be considered, except for low and very low voltage electrical cables and equipment or materials protected by housing or by a cabinet.
- Limitation of fire spreading using either the fire containment approach (fire compartments) in buildings separated into divisions or the fire influence approach (fire cells) in buildings or parts of buildings without divisional separation.
- A fire is assumed to occur during normal plant conditions (from full power to shutdown condition) or in a post-accident condition once a controlled state has been achieved or no sooner than two weeks following an earthquake.
- In order to be able to set up the suitable protective measures, the fire load for each room must be calculated and kept up-to-date.
- The temporary or permanent storage of fire loads during the various states of the plant as well as workshops with fixed, hot working work stations, must be identified and subject to risk analysis.
- The fire protection provisions must be optimised in order to limit the discharge of toxic or radioactive materials.
- The random failure of an active equipment item of the fire protection systems must not lead to a common mode failure on the systems needed to perform the F1 safety functions, even if these functions are not needed following such an event. The redundancy requirement (whether functional or not) due to this principle being taken into account must be implemented within the train separation principles.
- A check on the robustness to a random failure must be applied on a deterministic basis in the event of:
    - A fire independently of the accidents, liable to impair the integrity of the fire barriers,
    - A fire leading to PCC-2 events,
    - A fire resulting from a PCC-3/PCC-4 event.
- The random failure must be applied on a deterministic basis:
    - To the active equipment of the fire protection mechanical systems,

  - o To all the components of the fire protection electrical systems.

- A localised loss of integrity of the fire safety barriers may be accepted insofar as the failure of an active equipment item of the fire protection systems does not lead to a common mode on the systems required to perform F1 safety functions

7.1.3. Applicable regulations and design codes

7.1.3.1. Regulations

All applicable UK regulations must be considered.

7.1.3.2. Design Codes

The applicable design code is ETC-F (see Sub-chapter 3.8).

7.2. DESIGN BASIS [REF-1]

Provisions for protection against fire risks must be taken to:

- limit the spread of a fire,
- protect the safety functions of the facility,
- limit the propagation of smoke and the dispersion of toxic, radioactive, inflammable, corrosive or explosive materials,
- ensure the achievement of a safe state, personnel evacuation and all other necessary emergency actions.

These provisions involve implementing means of fire prevention, surveillance, fire fighting and limiting fire consequences, appropriate to the risks inherent to the facility. They are defined and justified on the basis of a study of the fire risks specific to each facility and its environment. The risk analysis is intended to optimise the level of protection under technically feasible conditions and demonstrate that the risk due to fire is ALARP.

The design of the fire protection systems is based on three types of measures, which are based on the three levels of protection (prevention, detection and extinguishing).

The three types of measures are as follows:

- Prevention,
- Containment,
- Control.

For each of these measures, it must be confirmed that an independent random failure will not cause failure of the fire protection safety objectives.

7.2.1. Prevention

Prevention comprises a set of measures, aimed at preventing the fire from starting or reducing the likelihood of a fire.

The requirements covering prevention are as follows:

- The preventive measures must, as a priority, deal with limiting the combustible material inventory, separating or shielding them (enclosure or cabinet) and preventing potential ignition sources from being placed near combustible materials.

- Preference must be given to the use of non-combustible materials (Euro-class A1 or A2s2d0).

If not class A1 the material must at least be type B or C and must not produce dense or toxic smoke.

7.2.2. Containment

If a fire starts, despite the preventive measures in place, measures must be taken to limit its spread and to prevent:

- impact on the function of the F1 systems. Fire damage must be restricted to one redundant train in a given F1 system.

- spreading to other rooms and into emergency exits and disrupting any fire fighting provisions.

- environmental impact contravening applicable UK Regulations.

Limiting the spread of a fire is achieved by dividing the buildings into fire compartments, which use physical or geographical separation principles.

Any installed fire barrier must contain the fire so that only one of the redundant trains in a given F1 system may be endangered by the fire, for cases where different redundant systems are installed in different areas, fire compartments or fire cells.

The requirements for separation are as follows:

- All safety classified buildings must be separated from other buildings using (R)EI 120 classified walls.

- Priority must be given to physical separation. In the same way, priority must be given to structural measures (fire resistance of the structures) rather than to reliance on fire protection devices.

- In case of fire, the redundant elements in a F1 system must be protected so that failure is limited to a single train.

- Random failure is only to be considered for active equipment items such as fire stop check valves and servo-controlled doors. Fire doors themselves, smoke extraction ducts and floor drains are considered as passive equipment items that are not subject to the random failure requirement.

- The following table summarises the different types of fire compartments:

Objective	Fire compartment
Radioactivity containment	Type 1a/b
Safety	Type 2
Protected evacuation route	Type 3
Facilitation of the intervention and limiting the unavailability	Type 4
Storage	Type 5

- The principles used take into consideration geographical separation (extinguishing – screen – distance). The containment is justified by taking into account the location of the concentrated heat loads and the combustible material properties. Fire cells must only be used in exceptional circumstances and their effectiveness must be demonstrated on both, fire propagation and radioactive or toxic waste release level.

- Where geographical separation is used, it will be justified by a vulnerability analysis as shown below

7.2.3. Fire compartment

There are five compartment types [Ref-1]:

Fire containment compartment (CCO / SFC) (Type 1a). These compartments are created when a fire in a safety building could lead to the release of radioactive or toxic materials which, in the absence of any dispersion measures outside of the relevant fire compartment causes deviation from acceptable release levels. In addition to containing the fire, they ensure the control of the released radioactive or toxic materials. The partitions of these fire and containment compartments must have a fire resistance rating (R)EI 120 and S200C5 classified doors [Ref-2]. They must also be fitted with a fixed automatic fire-extinguishing system capable of accomplishing its function in the event of a random failure.

Fire environment compartment (CEO / SFE) (Type 1b). These compartments are created when a fire outside a safety building could lead to the release of radioactive or toxic materials which, in the absence of any dispersion measures outside of the relevant fire compartment causes deviation from acceptable releases. In addition to containing the fire, they ensure the control of the released radioactive or toxic materials. The partitions of these fire and containment compartments must have a fire resistance rating (R)EI 120 and S200C5 classified doors. They must also be fitted with a fixed automatic fire-extinguishing system.

Safety fire compartment (SCO / SFS) (Type 2). These compartments are created to protect safety trains from common mode failure. The partitions of these safety fire compartments must have a fire resistance rating (R)EI 120 and S200C5 classified doors. For the UK EPR, the integrity of these fire barriers is maintained without claiming any credit from fire extinguishing systems [Ref-3] [Ref-4].

For the UK EPR, a door monitoring system (see section 6 of Sub-chapter 9.5) will be used to detect if a door installed within the boundary of a safety fire compartment is left open and will raise adequate alarms to alert the operator to an open door. The doors, which will be equipped with monitoring devices, contribute to the following safety functions:

- separation between buildings,
- divisional separation,
- segregation of safety trains.

The door monitoring system is not credited in the safety studies.

Access compartment (RCO / SFA) (Type 3). These compartments are intended to enable the personnel to be evacuated in full safety in the event of fire, and to provide access for fire-fighting teams. They corresponds to protected rescue routes. The partitions of these compartments must have a fire resistance rating equal to MAX (fire resistance of the adjacent fire area - (R)E 60) and the doors must be classified S200WC5 (smoke-tightness, limited radiation, durability in accordance with standard NF EN 13501-2). These compartments must not contain safety equipment or combustibles.

Intervention fire compartment (IFC / SFI) (Type 4). These compartments are created when the installation conditions result in the possibility of a flash over fire (PFG), to facilitate the intervention of fire fighting crews and limit unavailability of the unit. The partitions of these fire compartments must have a fire resistance rating suited to the consequences of the fire in the area without being less than (R)EI 60.

The size of these compartments must be consistent with these objectives and, wherever possible, the same IFC should not be used to cover several building floors.

It may be:

- included in a safety fire compartment,
- independent of any safety fire compartment.

7.2.4. Fire cells

In some buildings, and in the reactor building in particular, division into fire compartments may be limited due to construction or process factors, e.g.:

- Compact nature of the installation,
- Hydrogen concentrations,
- Steam releases in case of pipe break (rupture).

In this instance, some sections of the buildings may be divided into fire cells, where equipment is protected by spatial separation rather than physical barriers. Evidence of non-propagation of fire and avoidance of failures of safety classified equipment, must be established by assessing all possible modes of fire propagation and combustion products.

This geographical separation implies:

- A sufficiently low heat load or specific border conditions or an automatic extinguishing device. The first two principles will be specified during integration of the new thermal programme for fire assessment.

- Demonstration that it is not feasible to build a wall.

There are three fire cell types:

The safety fire cell (SCE / ZFS) (Type 2). These cells are created inside a safety fire compartment to protect safety functions from common mode failure. The boundaries of these safety fire cells must ensure the integrity of safety functions during the time needed to extinguish the fire. Active or passive fire protection means must be established if necessary.

The unavailability limitation fire cell (ULF / ZFI) (Type 4). These cells are created when the installation conditions imply the possibility of a localised fire, to limit the unavailability of the unit and facilitate the intervention of fire fighting crews

The storage cell (SC / ZS) (Type 5). These cells are created in the design phase to enable the operators to store equipment and materials required for operation, when the unit is at power or shut down. These cells are fitted with fire prevention, detection and fighting means, if necessary.

7.2.5. The non-contained areas

Non-contained areas (VNS) are created to identify rooms or groups of rooms not subject to fire containment for safety or security, to ensure that all rooms have been subject to a vulnerability analysis. They are used to control the fire parameters of the rooms making them up.

7.2.6. Physical separation

Separation is performed by the creation of fire compartments or by the use of fire-qualified passive protection features. The fire resistance of these protection devices must be at least equal to the duration of the reference fire, defined by the combustion of materials contained in the room and outside the enclosure, but not less than the duration of the fire in the compartment or cell with the longest fire duration.

Where it is not possible to shield part of the equipment in a room from a fire, fire retardant paints can be used on the condition that all the combustible materials present are also coated.

7.2.7. Geographical separation

The separation is achieved by creating fire cells or by using fire resistant geographical protection.

Geographical separation is combined with a fire risk analysis which concludes that the time required for the fire to reach the equipment is greater than the time required to extinguish the fire.

7.2.7.1. Distance

The use of physical distance ensures that a localised fire cannot propagate towards other combustible material. This is achieved by installing the combustible materials in such a way that the space between them is free from combustible material. Distance may also be used to prevent a fire causing failure in two redundant items of equipment. This is achieved by ensuring that there is sufficient distance between the combustible material and at least one of the redundant items for damage to be avoided.

The distance required depends on the direct radiated heat and the time required for the fire to reach other combustible materials or the equipment to be protected.

As a large number of parameters (type of combustible, location in the room, severity of the heat load, etc) are involved, it is difficult to define a general rule and as such the measures used are subject to specific assessments.

7.2.7.2. Thermal screen

This measure, which may be used to supplement protection by distance, enables equipment to be shielded from direct radiated heat. A screen is installed whose fire resistance is sufficient to withstand the severity and duration of the reference fire.

7.2.7.3. Fixed automatic protection associated with geographical separation

An additional means of protection, when the previous provisions (screen, distances) are not adequate, is provided by installing a fixed and automatic fire fighting means, which ensures that the fire will be extinguished or restricted before it reaches another combustible mass or two redundant items of equipment.

7.2.8. Control of fire

Detection and fire fighting devices are installed to detect and fight the fire and to control the fire as quickly as possible.

The control requirements are as follows:

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

7.2.9. Vulnerability analysis

Where a fire is detected, in a safety fire compartment or in a safety fire cell, operational failure of all the equipment is assumed (apart from those items of equipment which are protected by an approved fire barrier that is designed to resist the consequences of a fire).

The vulnerability analysis must either demonstrate that common mode failures [Ref-1] due to fire have been eliminated or show that the consequences of the postulated fire are acceptable.

As a general rule, the effects of fire are limited to the investigated fire area, whether it is a compartment, a cell or a division. For cells, the analysis is also conducted between adjacent cells.

The analysis is conducted in four steps:

Step 1 - search for potential common mode failures

A potential common mode failure is identified when the same fire safety volume (compartment or cell) contains the following:

a. safety-classified mechanical equipment or electrical connections belonging to two redundant trains of the same system performing a safety function,

or

b. safety-classified mechanical equipment or electrical connections belonging to one redundant train of a system performing a safety function, and the systems required to operate the redundant system,

or

c. electrical connections which do not belong to the previous categories but:

  - o which are power-supplied by redundant electrical switchboards and
  - o the train is such that the selection of the protective features on the switchboards may result in more than one train being affected.

Criterion c) relating to the non-selectivity of the electrical protective features is to be taken into account only when a fire may simultaneously affect both electrical trains (only the electrical connections present in the same room are therefore taken into account).

or

d. equipment whose failure in the event of fire is likely to result in a PCC situation and equipment required for the management of the situation,

or

e. Equipment whose failure is postulated with regard to the single aggravating factor in a PCC condition and equipment required in the study of the condition under consideration from the controlled state,

or

f. For all RRC-A and RRC-B conditions considered, a check will be performed that a fire does not prevent the final state being maintained beyond the 15 days following the initiating event.

Step 2 – functional analysis

Functional analysis of the consequences of the loss of equipment from step 1. This analysis provides a list of common modes which have been functionally confirmed.

In the event of fire in a division, special attention must be paid to protection of:

- interconnections to avoid spread of the fire into another division
- IRWST (RIS pool) to ensure its integrity

The analysis of the equipment required to return the plant to a safe state should be carried out taking a single aggravating factor into account (for PCC situations analysis).

Step 3 – analysis of fire risks

The fire risk analysis with respect to the treatment of potential common modes is based on the study of:

- Direct radiated heat,
- The time needed for the hot gases zone generated by the fire to reach the second fuel mass or the equipment to be protected,

Given the large number of parameters (nature of the fuel, geographical location in the room, concentration of the fire load, equipment malfunction temperature, etc.) involved in this demonstration; the analysis must be carried out on an individual basis using pre-defined failure criteria, depending on the type of equipment associated with the actual malfunction criteria of equipment [Ref-2]. If the use of a computer code is needed for the demonstration, the EDF MAGIC code will be used [Ref-3] [Ref-4]. This analysis provides a list of confirmed common modes.

Step 4 - treatment

When the analysis of step 3 confirms the existence of a common mode or the unacceptability of the loss of an item of non-redundant equipment, it is necessary to set up additional fire protection measures (wrapping, layout modifications,…).

7.2.10. Safety of personnel, evacuation, intervention

The term "rescue route" includes protected and non-protected rescue routes.

Rescue routes needed for the emergency evacuation of plant personnel must comply with appropriate UK codes and standards.

The protected rescue routes must have dimensions which are established according to the number of people passing through and the emergency means liable to be used (fire extinguishers, stretchers, etc).

Principles

(1) Buildings which present a significant fire risk must feature, a number of separate, protected rescue routes enabling personnel evacuation and the access by the emergency teams.

(2) These rescue routes constitute, themselves, by the limits provided by the walls of their fire compartments to ensure:

- o the evacuation of the personnel and injured persons in complete safety.
- o easy access for intervention teams with the means required to succeed in their mission.

(3) The access routes of the plant personnel from the control room to other rooms containing equipment important for the safe shutdown of the reactors must be protected rescue routes.

Evacuation and rescue routes

(1) Along the rescue routes, the doors must be capable of being opened even in the event of loss of power and the control facilities such as the turnstiles must be able to be bypassed in the event of evacuation.

(2) The rescue routes must emerge on the outside of a building or into a protected rescue route.

(3) The reactor building rescue routes must emerge into air locks. The latter must be operable in the absence of power, and both doors must be capable of being opened at the same time during unit outages.

(4) Rescue routes leading from a non-controlled area to a controlled area or leading directly out of a controlled area, are not generally allowed.

(5) The use of muster areas must, wherever possible, be limited.

7.2.11. Fire control (detection and fire fighting)

(1) Detection aims at being able to rapidly detect the start of a fire, locate it, initiate an alarm and in some cases initiate automatic actions. A safety related fire detection system is classified F2.

(2) The fire detection system must be operational in all the situations for which a fire is assumed to occur.

(3) The fire detection equipment is electrical equipment. Random failure must therefore be taken into account for all the detection equipment which is required for safety reasons.

(4) Pumps and control valves are active equipment items, the random failure of which must be taken into account. The pipework of the water circuits and sprinklers are considered passive equipment items. Failure to open simple dampers (swing dampers for example) does not need to be taken into account. Failure to close results in incomplete leak-tightness (partial leakage).

7.2.12. Consideration of random failure

The following active equipment is to be considered for a (single) random failure:

- Containment: fire stop devices (i.e. fire dampers).

- Detection: main detection equipment (as the detectors and their circuits are electrical equipment).
- Extinguishing: pumps, controlled valves that change position when the systems and sprinklers are activated.

When the redundancy of equipment (and its support systems), as well as any additional measures consisting of geographical or physical separation, and redundancy in electrical supply cannot be implemented, a minimum operational redundancy must be ensured.

7.3. STRUCTURAL FIRE PROTECTION MEASURES

7.3.1. Construction provisions

Construction provisions including installation for fire protection components and equipment must conform with ETC-F (see Sub-chapter 3.8).

7.3.1.1. Prevention

Limitation of combustible materials

The limitation of the potential fire risk is obtained by:

- The use of equipment and fluids, which are of limited combustibility and by limitation of their masses.
- Provisions to avoid the contact of pipes (carrying inflammable fluids with other materials or plant. It is forbidden to lay electrical cables less than 1m from any such pipes, other than those required to monitor or supply the equipment mounted on them.
- The use of class A1, A2, B and C materials having a low smoke generation index.

The use of combustible materials in dry nuclear fuel storage rooms is strictly forbidden.

7.3.1.2. Fire containing

The fire stability of load bearing elements, structure and walls of buildings (pillars, beams, floors, walls, etc.) must be at least two hours for the safety classified buildings.

Domino effects between adjacent buildings must be avoided by leaving a sufficient space between them or by inserting barriers with a suitable fire rating.

7.3.1.3. Characterisation of the walls of fire cells

The fire resistance characteristics of the walls of a fire area are defined by applying the EPRESSI method to each room, with at least one wall at the limit of the fire area. The fire resistance must not be less than the classification requirement defined in ETC-F.

Openings needed for pressure relief are permitted in separation structures which fulfil a fire protection role. In this case, these openings must be either automatically closed in the event of fire or opened only in the event of overpressure.

Ventilation ducts and pipes must not be paths for fire propagation between fire areas, whether or not they are fire compartments.

Electrical or mechanical penetrations through fire walls must be sealed with a suitable fire rated material.

If a ventilated cable and pipe tunnel is divided into fire compartments, transfer openings must be fitted with fire dampers.

7.3.1.4. Characterisation of common mode equipment inside fire safety compartments

A fire safety compartment must not contain equipment vulnerable to common mode failure (i.e. failure involving loss of elements of a safety system belonging to more than one safety division).

If this objective cannot be achieved, passive protection systems must be provided, the fire performance capability of which are appropriate to the characteristics of the reference fire assessed using the EPRESSI method, without being less than P120.

7.3.1.5. Characterisation of common mode equipment between fire safety cells

It was defined in the design section above that a fire in a fire cell must not spread to another fire cell or at the very least not cause a common mode failure as a result of fire propagation phenomena. This demonstration is carried out using detailed information on the installation, design, fuel load and the available fire detection and fire-fighting means.

7.3.1.6. Provisions against external fire

The on-site fuel material storage zones must be separated from the nuclear island buildings by a sufficient distance or by a fire wall with a fire rating sufficient to avoid any propagation.

Penetration of smoke and hot gases into buildings containing the safety equipment through the ventilation systems must be prevented.

7.3.1.7. Survey of fire loads

A room-by-room survey must be made of all fire loads and the elements required for the fire risk analysis (see section 7.2.9 – Step 3 – analysis of fire risks). If necessary, they must afterwards be grouped by fire area. The following fire loads must not be taken into account in the risk analyses due to the following reasons:

- If they are located inside components such that their ignition is impossible, even in the event of external fire, or
- Depending on the possible internal or external ignition sources, the components are in a position to withstand the load in normal operation and to retain their operability in the event of postulated accidents (including fire), or
- If it could be shown that the drainage of liquid fuels is possible, despite the effects of the fire.

7.3.2. Provisions for personnel safety

7.3.2.1. Location and accessibility of buildings

The access and operation areas needed for the fire and emergency services and for the deployment of the fire-fighting means must be designed and laid out so that the machinery can move without difficulty, including the use of aerial ladders if necessary.

Fire access points to safety buildings must be provided by at least two independent roads.

In the event of fire, it must be possible to keep open the access points for the emergency services and firemen. This is also applicable to the internal access points between building zones.

Accesses to buildings must be, wherever possible, be provided so that the emergency services and firemen and their fire fighting equipment required can be brought quickly to the scene of the fire.

The access doors for the emergency services and the fire suppression operations must be capable of being fully opened in the direction of evacuation. An exception may be made if necessary for the prevention of sabotage or in response to the process of some items of equipment (example: vacuum ventilation compartment) if the doors are infrequently used.

7.3.2.2. Escape routes

The current design is based on French regulations and standards. An assessment of the escape routes in accordance with applicable UK standards will have to be performed.

7.3.2.3. Smoke protection

Protected rescue routes and muster areas must be protected against smoke.

This protection is provided by the means described below (or a combination of such means):

- the mechanical or natural scavenging of fresh air.
- the pressure drop created in the affected room, once the smoke control system is put into operation.
- The design of the ventilation systems, which ensures that rescue routes are kept in slight overpressure with respect to the adjacent rooms (rooms liable to release large quantities of smoke in the event of fire) and through the cold smoke-tightness afforded by the doors.

7.4. DESIGN VERIFICATION [REF-1] TO [REF-8]

The methodology of the design verification is described in section 7.2.9 of this sub-chapter.

8. PROTECTION AGAINST INTERNAL FLOODING

8.1. SAFETY REQUIREMENTS AND DESIGN BASIS

8.1.1. Initiators and plant conditions

Internal flooding may damage essential equipment or civil structures and prevent the correct operation of safety related equipment.

The following potential initiators of internal flooding are considered in the assessment against internal hazards:

- Leaks and breaks in fluid systems
- Incorrect system configuration,
- Flooding by water from neighbouring buildings,
- Spurious operation of the fire extinguishing system, and use of mobile fire fighting equipment,
- Overfilling of tanks,
- Consequences of failure of isolation devices,
- Operator error.

External sources of flooding including snow and rain are covered in the external flooding assessment (see Sub-chapter 13.1).

In section 5.1.2.1 of Sub-chapter 13.1, related to external flooding, three of the hazards considered may originate within the reactor site and therefore constitute internal hazards, according to the definition given in section 1.1 these are as follows:

- deterioration of water channel structures : structures such as reservoir ponds, cooling towers basins that may exist within the site boundary
- breaks in systems or equipment : this hazard includes breaches in the CRF (circulating water system) in the turbine building, or breaches in non-seismically qualified site tanks following an earthquake.
- swell: the sudden trip of the CRF pumps (circulating water pumps) must be considered. Though originating on site, this hazard has to be considered in combination with high heat sink water levels, and thus is assessed together with external flooding.

According to the deterministic approach [Ref-1]:

- The initiators listed above must be considered; however only one of the initiators is postulated to occur at any one time, unless two or more initiators have a common identified cause.
- The flooding is expected to occur during normal operation of the reactor (during power operation or during shutdown). However assessments are also made against the most onerous plant conditions.

8.1.2. Flooding consequences

The systems and structures which are liable to fail during flooding are:

- all electrical and I&C equipment, with the exception of cables whose terminals are not flooded and where the equipment is protected against water ingress,
- certain civil structures that are not qualified to resist the floodwater pressure or its temperature,
- all non-watertight mechanical equipment.

8.1.3. General assumptions

8.1.3.1. Specifics concerning initiators

The specifics of the potential initiators listed in section 8.1.1 of this sub-chapter are given below:

8.1.3.1.1. Flooding caused by leaks and breaks in fluid systems

The failure assumptions are described in section 2 and section 3 of this sub-chapter

8.1.3.1.2. Incorrect system configuration

In general, flooding due to a configuration error is prevented by procedural means. However, these potential sources are analysed by taking into consideration the operational experience from existing units.

8.1.3.1.3. Flooding by water from neighbouring buildings, and in other outside water capacities or ducts on the site.

This potential source of flooding must be avoided by separation and segregation measures to prevent indirect flooding into safety-classified buildings.

8.1.3.1.4. Spurious operation of the fire fighting system

This must be considered in the flooding analysis. The effects of flooding caused by mobile fire fighting systems must also be assessed.

8.1.3.1.5. Overfilling of tanks

This must be taken into consideration during the design of level measuring devices, sumps and isolation components.

8.1.3.1.6. Consequences of failures of isolation devices

Provision must be made for double isolation, if necessary.

8.1.3.2. Leak duration

The following approaches concerning leak duration must be applied:

- If the breach can be detected by the I&C systems, and if provision has been made for automatic isolation, the release time is determined by the time taken to detect the leak plus the time taken to actuate the automatic isolation.
- If the breach can be detected by signals in the main control room, and if provision is made for manual isolation from the main control room, the release time comprises the time taken for the first alarm to be received in the control room plus a nominal 30-minute period allocated to manual actions in the main control room.
- If the breach can be detected by signals in the main control room, and if provision is made for isolation using local actions, the release time comprises the time taken for the first alarm to be received in the control room plus the time allocated to the operators for performing the local action: for example for manual isolation of a valve it is assumed that the time allocated to a local action is 1 hour.
- If the breach cannot be detected or if isolation is not possible, the release of the full inventory of the failed system is assumed, if the leakage is not limited in another way.

For the divisional segregation verification (section 8.2, step 1), the analysis has been performed on the basis that the most onerous human actions (local action or action from the MCR) required to ensure that the flood volume is limited to the retention volume available within the building are supported by “Task Analyses” (see Sub-chapter 18.1), to show that they can be achieved with adequate reliability within the available time.

8.1.3.3. Volumes of released water

If isolation of a breach is assumed, only the volume of water released during the period up to isolation is considered. The content of the part of the system which cannot be isolated is assumed to be released.

For the purposes of estimating the leakage flows, the maximum operational pressure is generally considered.

All feeds to the pumps (including the injection flows from other systems) are considered.

Any released steam is considered to be fully condensed.

8.1.3.4. Installation considerations

The design of the facility includes adequate provision for the collection and discharge of water reaching the site from any design basis internal flooding hazard. Where this is not achievable, the structures, systems and components important to safety will be adequately protected against the effects of water. Such measures include:

- The water may flow to the lower levels via the stairwells, lift wells, the building's drainage system or other openings.
- The sump pumps of the building drainage system are pessimistically considered as unavailable.
- It is assumed that the level of water is equally distributed in all of the zones concerned, at the lowest level.
- Walls in the interface and periphery of the Nuclear Island buildings have been sized to withstand a 10 m water column from the basement level.
- The doors at the interfaces of the buildings and divisions are resistant to the maximum water column resulting from the main initiating event or the initiating event used for the sizing of the civil works. These doors are qualified for the resulting requirements. Similarly, the materials used for caulking, to close the openings and the joins in the walls between the divisions, are qualified against the water column height of the main initiating event.
- With regard to the room in which the water is released, the level may be higher in the case of high flows. It must only be considered for specific instances where the systems/equipment to be protected are located in these rooms.
- The flood barriers for safety-classified equipment are taken into consideration.

In order to minimise the effects from an internal flooding event, the design and layout of the site and its facilities are such that they:

- Minimise the direct effects of internal flooding on structures, systems or components;
- Minimise any interactions between a failed structure, system or component and other safety-related structures, systems or components;
- Ensure site personnel are physically protected from direct or indirect effects of incidents;
- Facilitate access for necessary recovery actions following an event.

Support facilities and services important to the safe operation of the reactor are designed and routed so that, in the event of incidents, sufficient capability to perform their emergency functions will remain. Support facilities and services include access roads, water supplies, fire mains and site communications.

8.1.4. Installation rules

8.1.4.1. Floods which are initiated in category 1 buildings (except the nuclear auxiliary building and effluent treatment building)

In buildings which are split into divisions, the complete loss of a division does not prevent fulfilment of the essential safety functions. Therefore, the main safety objective is to ensure that an internal flood cannot extend to another safety-classified building or another safety classified division. However, certain other additional measures may be necessary, for example:

- Isolating the RIS [SIS] sump valves in case of failure in RIS [SIS] pipework, in order to protect the IRWST supply,
- Protection of the main control room against flooding originating from the chilled water system (DEL) located above.

In the other buildings (reactor building, fuel building) flooding must be prevented from causing failure in redundant F1 systems (including the support systems). If necessary, mitigation measures must be taken, such as:

- The construction of local partition walls between the system's redundant section in the non-divided areas,
- Locating the components at higher levels,
- Reducing the level of flooding using measures such as drains.

8.1.4.2. Floods initiated in nuclear auxiliary building, effluent treatment building, and in buildings which are not safety classified

In case of internal flooding in the nuclear auxiliary building or in buildings which are not safety classified but which are connected to safety classified buildings or any other flooding on site, water must be prevented from entering the safety classified buildings.

8.2. DESIGN VERIFICATION

The design verification for internal flooding is the deterministic demonstration that the unit has acceptable protection against such a hazard. It is carried out in two steps according to the methodologies described below.

Step 1: divisional segregation verification

This analysis provides a general demonstration that divisional segregation is maintained following the most severe flooding event in each building. The operator actions required to maintain divisional segregation are determined and identified as safety significant. The analysis comprises the following:

- The potential volume and flow rate of each flooding initiator in each building without any operator action is calculated.

- The retention volume is derived for the buildings which contain barriers to prevent the spreading of flood water to other buildings. In the Nuclear Island, basement levels ensure retention of flood water.

- Flooding initiators with the ability to jeopardise segregation are identified as major flooding events [Ref-1].

- For major flooding events, the operator actions required to prevent spreading of the flood to other buildings are identified, together with the available timescales. This assessment takes into account the Single Failure Criterion [Ref-2].

- A dedicated human factors analysis is performed (as described in Sub-chapter 18.1) for relevant cases in order to guarantee that the required operator actions are achievable within the timescales identified above [Ref-3].

This divisional segregation verification is performed in order to verify that divisional segregation is maintained even in the circumstance of a Double Ended Guillotine Break (DEGB) of moderate energy classified pipework with nominal diameter greater than 50 mm. A dedicated analysis, which uses realistic assumptions wherever justified, has been performed for the Reactor Building, Safeguard Buildings, Fuel Buildings and Diesel Buildings [Ref-4]. This analysis includes Human Factors aspects [Ref-3].

<u>Step 2 : detailed vulnerability analysis</u>

The analysis takes into account simultaneous effects, common cause failure, defence in depth and consequential effects. To achieve this, the analysis takes into account that:

- certain hazards may not be independent of internal flooding and may occur simultaneously or in a combination that it can be reasonably expected;

- an internal or external hazard may occur simultaneously with an internal fault, or when plant is unavailable due to maintenance;

- there is a significant potential for internal or external hazards to act as initiators of common cause failure, including loss of off-site power and other services;

- internal flooding events have the potential to threaten more than one level of defence in depth at once;

- internal flooding can arise as a consequence of faults internal or external to the site and should be included, therefore, in the relevant fault sequences;

- the severity of the effects of the internal or external flooding experienced by the facility may be affected by facility layout, interaction, and building size and shape.

This detailed analysis is performed at the end of the detailed studies, for each safety-classified building. The onset of a flood will be postulated for each room, for each applicable type of initiator. The consequences are assessed, using the assumptions presented in this sub-chapter.

The methodology for analysis of the internal flooding hazard for buildings making up the nuclear island [Ref-5] specifies the method for analysing the threat to essential plant items from internal flooding events, and is equally applicable to nuclear safety related buildings that are not part of the nuclear island.

For each building ([Ref-6] to [Ref-10]), the following aspects are assessed:

- The possible sources of flooding
- The water paths between various rooms
- Safety related equipment that can be affected by the consequences of internal flooding (such as flooding, spray, loss of a supporting system).
- Identification of possible common mode failures
- The risk of groundwater pollution/release of radioactive waste

Sensitivity studies are performed for certain initiating events in order to show the absence of any cliff-edge effects in terms of radiological consequences.

APPENDIX 1: HAZARD FAULT SCHEDULE PRINCIPLES

A1.1. GENERAL OBJECTIVE AND CLAIM

The Hazard Fault Schedule provides a compact summary of the safety case and studies addressing internal hazards, showing the derivation of safety functions and related safety features, together with their safety category and classification respectively.

The UK EPR Classification scheme (Safety Function Category A/B/C and Safety Class 1/2/3) from Sub-chapter 3.2 has been used in the representative examples [Ref-1], which illustrate how this methodology is applied respectively to a selected representative frequent and infrequent Internal Flooding initiating event, within the scope of generic design.

A1.2. BASIS OF THE HAZARD FAULT SCHEDULE

The format of the Hazard Fault Schedule is taken and developed from that used for the fault schedule, in PCSR Sub-chapter 14.7. The content is based on and developed from the hazards analyses available for the FA3 project, and also those produced specifically for UK EPR. Due to the numerous hazards studies and the impact of hazards on plant safety, it is necessary to adapt the fault schedule as described in the next section. It should be noted that, as detailed hazards analyses also require the detailed design of the plant, the level of detail that can be provided at this stage mainly emphasises the basic design of the hazards protection.

A1.3. DESCRIPTION OF THE SCHEDULE AND ARGUMENTS

There are four main components of the Hazard Fault Schedule, which are shown in a similar format to the fault schedule:

- Input to classification and hazards description;
- Safety functions;
- Safety Functional Groups (SFGs);
- Fault analyses.

These components are each described below.

A1.4. INPUT TO CLASSIFICATION AND HAZARDS DESCRIPTION

The main purpose of this part of the schedule is to:

- Present the hazard studied together with relevant reactor states and its frequency of occurrence (columns “reactor state”, “hazard description” and “frequency”);

- Identify representative bounding case(s) and, depending on the hazard, provide a description or a reference to the corresponding study (column “representative bounding hazard sequences”), and;

- Indicate the potential direct consequences of the hazard (column “Main potential consequences”).

No screening has been conducted to limit the number of hazards considered in the schedule. The intention is to show all relevant bounding hazards taken into account in the UK EPR design.

Potential direct consequences of the presented bounding hazard for a particular area (e.g. flooding in Safeguard Auxiliary Building, SAB, 1 or 4) are given based on the available hazards studies (e.g. “JPI failure resulting in flooding in SAB” and “break in the upper level compartments”). These hazards studies permit the resulting consequences of the hazard to be assessed and linked to a relevant fault initiating sequence (e.g. feedwater line break). The purpose of this is to limit the amount of duplicated information provided in the Hazard Fault Schedule. If a fault is identified, details of this are provided in the fault schedule only and not repeated in the Hazard Fault Schedule.

Furthermore, information on the relevant reactor state is provided in the column “Reactor state”, allowing screening of the bounding hazards on this basis. Nevertheless, it is considered that bounding hazard sequences are likely to occur in State A except for a number of specific hazards specifically relevant to shutdown states, such as load drops in the Reactor or Fuel Buildings.

A1.5. SAFETY FUNCTIONS

Safety Functions are derived and categorised against initiating events and their potential consequences to classified Structures, Systems and Components:

- Identify the relevant Plant Level Safety Function and Lower Level Safety Functions challenged;

- Identify the consequences of failure of the Lower Level Safety Functions;

- Propose a suitable category of Lower Level Safety Function.

In the context of hazard protection, two kinds of Plant Level Safety Functions (PLSF) may be considered. The first one is to prevent propagation of a hazard to unaffected divisions of the plant consistently with the safety requirements defined in the basic design of the EPR. This function corresponds mainly to a barrier role in buildings separated into divisions, which reflects the main safety principle for protection against hazards, i.e. segregation of redundant safety trains. The second kind of Plant Level Safety Function deals with mitigation of hazards occurring in buildings or parts of buildings that are not separated into divisions. In this case, the aim is to avoid losing more than one redundant safety train in the affected area.

The Plant Level Safety Functions are broken down into Lower Level Safety Functions (LLSF). The LLSFs indicate what must be achieved in detail to fulfil the PLSF. This allows subsequent identification of the Safety Functional Group (SFG) required to perform these safety functions.

Depending on the potential consequences in case of failure of a certain LLSF (column “main potential consequences in case of failure of the LLSF”), a category is allocated to the LLSF. This allocation of safety category is based on criteria defined in PCSR Sub-chapter 3.2.

A1.6. SAFETY FUNCTIONAL GROUPS

The purpose of this part of the schedule is to:

- Identify the safety functional groups ensuring the Plant Level Safety Functions;
- Identify the main structures, systems and components belonging to the safety functional groups (columns “safety feature description”), and;
- Assign each of these safety functional groups to a safety class.

As the detailed design of the plant is not yet available at this stage, it is not always possible to provide the relevant information for the systems, structures, and components (SSCs). The safety functional groups ensure that the correct safety class is allocated to the SSCs, even if the detailed design is not yet available.

The classification principles defined in PCSR Sub-chapter 3.2 are to be applied to these SFGs and further SSCs. A lower safety class than the one expected by the safety category may be appropriate. In such a case, it is made clear that the related SSCs play an auxiliary role in achieving the safety function. However, as a general rule, the main structures which ensure a Category A “barrier” safety function (in any of the Main Safety Function categories) should be Class 1, and any exceptions must be justified as ALARP.

A1.7. FAULT ANALYSES

The purpose of this part of the schedule is to identify a bounding fault sequence for each initiating event (or group of plant consequences), and relevant plant state, demonstrating that plant safety is ensured from a fault analysis perspective.

This part of the schedule makes a direct link between the hazard and the bounding fault from the fault schedule in order not to duplicate description of protection in terms of Category A safety functions for reactivity control, heat removal and confinement.

For frequent hazards (i.e. with an Initiating Event Frequency exceeding 10^{-3}/r.y), the table also references the bounding functional diversity analysis, which ensures that diverse means of protection are provided. These diverse analyses are also given in the fault schedule or in the RRC-A analyses. References are provided for further assessment. It should be noted that diversity is not required to be provided in terms of protection against hazard consequences themselves, only in terms of reactivity control, heat removal and confinement.

A1.8. CONCLUSIONS

The representative Hazard Fault Schedule [Ref-1] for internal hazards is designed to provide a logical and visible basis for the presentation of the safety case on which to base the site-specific case in a later revision during the site licensing phase.

The key safety case claims have been identified and appropriate arguments have been made, which are supported by evidence from the PCSR hazards study in the main body of Sub-chapter 13.2. It is therefore concluded that a robust representative safety case has been presented in a visible manner, demonstrating the generic approach in the UK EPR Generic Design towards design basis internal hazards.

SUB-CHAPTER 13.2 – 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.

2. PROTECTION AGAINST PIPEWORK LEAKS AND BREAKS

[Ref-1] Procedure ENG 2-98: High energy pipes leaks and breaks analysis methodology. ECEF041142 Revision B1. EDF. June 2009. (E)

ECEF041142 Revision B1 is the English translation of ECEF041142 Revision B.

2.1. SAFETY REQUIREMENTS

2.1.2. Requirements for protection against failures of pipework

2.1.2.1. Identification of risks

[Ref-1] Identification of High Integrity Components - components whose gross failure is discounted. ENSNDR090183 Revision D. EDF. October 2012. (E)

2.2. DESIGN BASIS

2.2.1. Definitions

[Ref-1] Break Preclusion in reactor main coolant lines and main steam lines. Positioning of the concept and associated safety requirements. ENSNDR080245 Revision A. EDF. (E)

ENSNDR080245 Revision A is the English translation of ENSN040134 Revision C

2.2.2. Failure assumptions for High Energy Pipework

2.2.2.1. High Energy Pipework

2.2.2.1.3. Prevention of High Energy Line Breaks and Leaks

[Ref-1] Determination of rupture locations and dynamic effects associated with the postulated rupture of piping. NUREG-0800 Standard Review Plan - 3.6.2 Revision 2. March 2007. (E)

[Ref-2] Protection Against Postulated Piping Failures in Fluid Systems Outside Containment. NUREG-0800 Standard Review Plan - Branch Technical Position 3-3 Revision 3. March 2007. (E)

[Ref-3] Postulated Rupture Locations in Fluid System Piping Inside and Outside Containment. NUREG-0800 Standard Review Plan - Branch Technical Position 3-4 Revision 2. March 2007. (E)

[Ref-4] Protection against internal hazards other than fires and explosions in the design of nuclear power plants. IAEA Safety Guide NS-G-1.11. 2004. (E)

2.2.3. Failure assumptions for Moderate Energy Pipework

[Ref-1] Design and Construction Rules for Mechanical Components of PWR Nuclear Islands. RCC-M. AFCEN. 2007 Edition. (E)

[Ref-2] Determination of rupture locations and dynamic effects associated with the postulated rupture of piping. NUREG-0800 Standard Review Plan - 3.6.2 Revision 2. March 2007. (E)

[Ref-3] Protection Against Postulated Piping Failures in Fluid Systems Outside Containment. NUREG-0800 Standard Review Plan - Branch Technical Position 3-3 Revision 3. March 2007. (E)

[Ref-4] Postulated Rupture Locations in Fluid System Piping Inside and Outside Containment. NUREG-0800 Standard Review Plan - Branch Technical Position 3-4 Revision 2. March 2007. (E)

[Ref-5] Protection against internal hazards other than fires and explosions in the design of nuclear power plants. IAEA Safety Guide NS-G-1.11. 2004. (E)

2.3. DESIGN VERIFICATION

[Ref-1] 1st stage analysis report on the consequences of a high-energy line break - Reactor Building. ECEF092040 Revision A1. EDF. April 2010. (E)

[Ref-2] Stage 1 analysis of consequences of high-energy line breaks in fuel building. ECEF092041 Revision A1. EDF. November 2009. (E)

[Ref-3] 1st stage analysis: consequences of a high-energy line break - safeguard auxiliary and electrical buildings. ECEF092042 Revision A1. EDF. February 2010. (E)

[Ref-4] Additional information for the stage 1 analysis report on the consequences of high energy line breaks – fuel building. ECEF101595 Revision A1. EDF. May 2011. (E)

[Ref-5] Additional information for the stage 1 analysis report on the consequences of high energy line breaks – safeguard auxiliary buildings. ECEF101596 Revision A1. EDF. May 2011. (E)

2.3.2. Analysis of overall consequences

2.3.2.3. Pressure, Temperature, Humidity

[Ref-1] High Energy Pipe Break: propagation of degraded ambient conditions in the nuclear island. EZLT/2010/en/0007 Revision B. EDF. August 2010. (E)

3. PROTECTION AGAINST FAILURES OF TANKS, PUMPS AND VALVES

3.2. DESIGN VERIFICATION

3.2.1. Classified equipment (M1 / M2 / M3 requirements)

[Ref-1] Identification of High Integrity Components - components whose gross failure is discounted. ENSNDR090183 Revision D. EDF. October 2012. (E)

4. PROTECTION AGAINST MISSILES

4.1. SAFETY REQUIREMENTS AND DESIGN BASIS

4.1.1. Selection and description of missiles

[Ref-1] Identification of High Integrity Components - components whose gross failure is discounted. ENSNDR090183 Revision D. EDF. October 2012. (E)

4.2. DESIGN VERIFICATION

[Ref-1] EPR – Internal Missiles – Risk assessment report on building structure and layout ECEIG091634 Revision B1. EDF. April 2011. (E)

4.2.2. Analysis for the reactor building

4.2.2.1. Missiles generated inside the reactor building considered in the analysis

4.2.2.1.1. Reactor vessel, steam generators, pressuriser, accumulators, reactor coolant pump body and other high energy tanks

[Ref-1] Identification of High integrity Components: components whose gross failure is discounted. ENSNDR090183 Revision D. EDF. October 2012. (E)

[Ref-2] Internal Missiles - Detailed analysis of the selected safety classified components gross failure. ECEIG112173 Revision A. EDF. January 2012. (E)

4.2.2.1.4. Reactor coolant pump flywheel

[Ref-1] Identification of High Integrity Components - components whose gross failure is discounted. ENSNDR090183 Revision D. EDF. October 2012. (E)

[Ref-2] Reactor coolant pump of EPR - Mechanical behaviour of the flywheel – dimensioning analysis. 6 CS 20099 Revision B. AREVA. November 2006. (E)

4.2.2.2. Protection against internally generated missiles

4.2.2.2.1. Barriers around the reactor coolant system loops

[Ref-1] EPR – Internal missiles – Methodology description for analysis of layout in the buildings – Conditions for preparing design reviews.
ECEIG070282 Revision A1. EDF. April 2010. (E)

4.2.2.2.2. Barriers around the pressuriser safety valves

[Ref-1] EPR – Internal missiles – Methodology description for analysis of layout in the buildings – Conditions for preparing design reviews.
ECEIG070282 Revision A1. EDF. April 2010. (E)

4.2.2.2.3. Barriers above the Control Rod Drive Mechanisms (CRDMs)

[Ref-1] EPR – Internal missiles – Methodology description for analysis of layout in the buildings – Conditions for preparing design reviews.
ECEIG070282 Revision A1. EDF. April 2010. (E)

4.2.2.2.4. Arrangement of containment isolation valves

[Ref-1] EPR – Internal missiles – Methodology description for analysis of layout in the buildings – Conditions for preparing design reviews.
ECEIG070282 Revision A1. EDF. April 2010. (E)

4.2.3. Analysis for the safeguard buildings

4.2.3.2. Missiles generated inside the safeguard buildings

4.2.3.2.3. Main steam feed water valve compartments

[Ref-1] EPR – Internal missiles – Methodology description for analysis of layout in the buildings – Conditions for preparing design reviews.
ECEIG070282 Revision A1. EDF. April 2010. (E)

4.2.4. Analysis of the fuel building

4.2.4.2. Missiles generated inside the fuel building

[Ref-1] EPR – Internal missiles – Methodology description for analysis of layout in the buildings – Conditions for preparing design reviews.
ECEIG070282 Revision A1. EDF. April 2010. (E)

5. PROTECTION AGAINST DROPPED LOADS

5.2. DESIGN BASIS

5.2.4. Operational rules

[Ref-1] UK EPR GDA - Management of Nuclear Safety Significant Lifting.
ECEMA101802 Revision B. EDF. December 2010. (E)

5.3. DESIGN VERIFICATION

5.3.1. Non-classified and Additional Requirements Equipment

[Ref-1] EPR - Load drops - Methodology for risks analysis in civil engineering and building installations - Design review preparation conditions.
ECEIG070272 Revision A1. EDF-SA. March 2009. (E)

[Ref-2] Methods with regard to the risk of "dropped loads" for EPR UK for civil works structures.
ENGSGC100483 Revision B. EDF. February 2012. (E)

[Ref-3] Safety case of four representative load drops from RS2 cranes.
ECEIG120198 Revision A. EDF. February 2012. (E)

[Ref-4] Identification of Dropped loads and Fuel Handling Human Based Safety Claims - Refuelling Machine.
PEPS-F DC 135 Revision B. AREVA. July 2012. (E)

5.3.2. Higher Requirements Equipment

[Ref-1] ALARP Justification of representative Drop Load Cases from SC1 polar crane.
PEPS-G/2011/en/1076 Revision C. AREVA. February 2012. (E)

[Ref-2] Identification of Dropped loads and Fuel Handling Human Based Safety Claims - Polar Crane.
PEPS-F DC 134 Revision B. AREVA. June 2012. (E)

6. PROTECTION AGAINST INTERNAL EXPLOSIONS

[Ref-1] Internal explosion methodology report.
ECEIG060350 Revision A1. EDF. February 2009. (E)

ECEIG060350 Revision A1 is the English translation of ECEIG060350 Revision A.

6.3. DESIGN VERIFICATION

6.3.2. Analysis of the risks of explosion in the Nuclear Island

6.3.2.1. Prevention of the risks of explosion

6.3.2.1.5. Risk of explosion inside systems

[Ref-1] Analysis of operational experience feedback concerning hydrogen-related explosions in safety-classified buildings at nuclear power plants in France and abroad, as applied to the EPR. ECEIG070648 Revision A1. EDF. October 2008. (E)

6.3.2.2. Analysis of the consequences of an explosion inside the nuclear island buildings

[Ref-1] Identification of systems and rooms in the EPR nuclear island (BNI) with risk of internal explosion. EYRL/2007/fr/0036 Revision H1. EDF. April 2011. (E)

6.3.2.2.3. Study assumptions

[Ref-1] B. Gautier. Reference base for safety requirements concerning protection against the risk of internal explosion for the EPR.
ENGSIN080356 Revision A. EDF. March 2009. (E)

ENGSIN080356 Revision A is the English translation of ENGSIN060237 Revision A.

7. PROTECTION AGAINST FIRES

[Ref-1] Fire methodology report. ECEIG0100658 Revision C1. EDF. February 2009. (E)

7.2. DESIGN BASIS

[Ref-1] M Mosse. EPR Technical code for fire protection. ETC-F Version G.
ENGSIN050312 Revision B. EDF. August 2007. (E)

7.2.3. Fire Compartment

[Ref-1] M Mosse. EPR Technical code for fire protection. ETC-F Version G.
ENGSIN050312 Revision B. EDF. August 2007 (E)

Fire containment compartment (CCO / SFC) (Type 1a).

[Ref-2] Fire classification of construction products and building elements – EN 13501-2:2003. (E)

Safety fire compartment (SCO / SFS) (Type 2).

[Ref-3] Fire Safety Assessment of Safety Fire Barriers - Evaluation of fire resistance using experience of comparable EPR layouts. NESP-G/2009/en/1322 Revision C. AREVA. March 2011. (E)

[Ref-4] UK EPR – MAGIC simulation for one representative safety compartment (SCO) and comparison with standard resistance curves without taking credit for active fire protection systems. ECEIG091608 Revision A. EDF. September 2009. (E)

7.2.9. Vulnerability analysis

[Ref-1] Principle of common mode fire risk analysis ENSNEA090055 A. EDF. July 2009. (E)

ENSNEA090055 Revision A is the English translation of ENSNEA070029 Revision A

Step 3 – analysis of fire risks

[Ref-2] Principle of the EPRESSI method. ENGSIN080155 Revision A. EDF-SA. May 2008. (E)

[Ref-3] MAGIC software version 4.1.1: Mathematical model. HI-82/04/024/B. EDF-SA. 2005. (E) This document contains EDF-SA proprietary information and can be accessed by direct contact with EDF SA.

[Ref-4] Qualification file of fire code MAGIC version 4.1.1. HI-82/04/022 Revision B. EDF. December 2005. (E)

7.4. DESIGN VERIFICATION

[Ref-1] Justification of fire zoning in the emergency diesel buildings at Flamanville 3. EYRL/2007/FR/0026 Revision D1. SOFINEL. August 2009. (E)

EYRL/2007/FR/0026 Revision D1 is the English translation of EYRL/2007/FR/0026 Revision D.

[Ref-2] Justification of fire zoning within the Flamanville 3 Fuel Building. EYRL/2007/FR/0020 Revision E1. SOFINEL. September 2009. (E)

EYRL/2007/FR/0020 Revision E1 is the English translation of EYRL/2007/FR/0020 Revision E.

[Ref-3] Justification of fire zoning within the Flamanville 3 Reactor Building. EYRL/2007/FR/0022 Revision E1. SOFINEL. August 2009. (E)

EYRL/2007/FR/0022 Revision E1 is the English translation of EYRL/2007/FR/0022 Revision E.

[Ref-4] Transverse Technical Studies Fire (Internal Hazard) – Studies by safeguard buildings 1/2/3/4 justification of the fire zoning.
EZL/2006/en/0082 Revision F. EDF. April 2009. (E)

[Ref-5] Verification of zoning fire resistance in waste building Flamanville 3. EYRT/2009/FR/0027 Revision B. SOFINEL. November 2009. (E)

[Ref-6] Verification of zoning fire resistance in Diesel buildings Flamanville 3. EYRT/2009/FR/0028 Revision B. SOFINEL. November 2009. (E)

[Ref-7] Preliminary analysis for verification of zoning fire resistance in fuel building. EYRL/2008/FR/0105 Revision B. SOFINEL. April 2009. (E)

[Ref-8] Location of cable trays in the EPR FA3 Nuclear Island EYRT/2010/FR/0042 Revision B1. SOFINEL. November 2011. (E)

8. PROTECTION AGAINST INTERNAL FLOODING

8.1. SAFETY REQUIREMENTS AND DESIGN BASIS

8.1.1. Initiators and plant conditions

[Ref-1] Protection of nuclear units against risk of external flooding. Methodological procedure for checking protection provisions.
ENSNEA090003 Revision A. EDF. February 2009. (E)

ENSNEA090003 Revision A is the English translation of ENSN0000850 Revision D.

8.2. DESIGN VERIFICATION

[Ref-1] Identification of bounding cases - leak volumes and retention volumes. ECEIG110718 Revision A. EDF. June 2011. (E)

[Ref-2] Bounding cases : mitigation measures. ECEIG111647 Revision B. EDF January 2012. (E)

[Ref-3] EDF/AREVA GDA Human Factors Internal Flooding. 16895-707-000-RPT-0013 Revision E. AMEC. September 2012. (E)

[Ref-4] UK EPR - Internal flooding - Multi-legged safety case and ALARP consequence assessment analyses.
ECEIG121115 Revision B. EDF. September 2012. (E)

[Ref-5] Internal flooding – Layout Analysis Methodology for buildings in the nuclear island. ECEIG040650 Revision C1. EDF. 2008. (E)

[Ref-6] Flooding Safety Analysis for Nuclear Auxiliary Building HNX PF2009EN0001 Revision D. SOFINEL. February 2011. (E)

[Ref-7] Flooding event : Analysis of the Safeguard Buildings EZT/2009/EN/0005 Revision E. SOFINEL March 2011. (E)

[Ref-8] EPR FA3 Fuel Building internal flooding assessment EYRT/2009/FR/0008 Revision C1. SOFINEL. November 2011. (E)

[Ref-9] Analysis of internal flooding in the FA3 EPR Reactor Building EYRT/2009/FR/0076 Revision D1. SOFINEL November 2011. (E)

[Ref-10] Study of Internal Flooding events in the Diesel Generator Building of the Flamanville FA3 EPR. EYRT/2009/FR/0032 Revision E1. EDF. April 2012. (E)

APPENDIX 1: HAZARD FAULT SCHEDULE PRINCIPLES

A1.1. GENERAL OBJECTIVE AND CLAIM

[Ref-1] UK EPR Hazard Fault Schedule – Representative Cases Based on Application of Hazard Fault Schedule Methodology.
ECESN120418 Revision A. EDF July 2012. (E)

A1.8. CONCLUSIONS

[Ref-1] UK EPR Hazard Fault Schedule – Representative Cases Based on Application of Hazard Fault Schedule Methodology.
ECESN120418 Revision A. EDF July 2012. (E)