SUB-CHAPTER R.1 LEVEL 1 PROBABILISTIC SAFETY ASSESSMENT

1. INTRODUCTION

This Sub-chapter is divided into three parts. The first two parts cover the PSA objectives and the methodology. The third part deals with the results, which are presented in terms of the core damage frequency per reactor per year (CDF).

The safety probabilistic objectives are described in Sub-chapter R.0.

1.1. OBJECTIVES

Probabilistic studies are carried out during the design process to support and optimise the design of systems and processes. This allows a well-balanced system and process design to be achieved. It also provides a reasonable assurance that plant will comply with the general safety objectives.

The risk quantification is carried out using RiskSpectrum© software. Fault trees are used to estimate the failure probability of the system missions. Event trees are used for estimation of the core damage frequency (CDF) for each initiating event.

1.2. SCOPE AND LIMIT OF STUDY

Level 1 PSA studies are the subject of this Subchapter. The results are presented in terms of CDF (/r.yr).

The model used provides satisfactory coverage of all potential accident situations related to the reactor. The scope of the probabilistic study is defined below:

- all reactor operational modes are covered, from operation at full power to refuelling shutdown with at least one fuel element in the reactor vessel;
- the study is limited to internal events only (except for loss of ultimate heat sink and loss of offsite power);
- thermal-hydraulic and neutronic parameters, initial conditions, set-points and component availabilities are based on realistic data.

1.3. CORE DAMAGE CRITERIA

In general, excessive clad temperature is used as the criterion for core damage in the thermal-hydraulics calculations.

In certain special cases, a primary pressure criterion may be used. In these cases it is assumed that a pressure higher than the limit would lead to a rupture of the primary system beyond the design basis.

The criteria are established by deterministic and bounding calculations.

2. METHODOLOGY

2.1. DATA

2.1.1. Assumptions: duration of various reactor operational modes

All reactor operational modes are studied in the PSA, from full power operation to refuelling shutdown with at least one fuel element in the reactor vessel.

The duration of the various reactor operational modes are evaluated by considering outages: these include programmed outages, forced outages, outages for start-up and planned tests, and outage extension either for specific work or due to organisational problems. The following assumptions are made concerning programmed outages: refuelling and maintenance outage duration: 16 days; turbine maintenance outage duration: 31 days; ten year inspections outage duration: 40 days.

2.1.2. Reliability data

Reliability data are derived mainly from operational feedback from France and Germany, supplemented by the EG&G generic reliability database.

Reliability data used for instrumentation and control systems are defined in Section R.1.2.2.

In general, data is chosen based on the existing French or German design that most closely matches the EPR.

In case of equivalence data from different sources, the most conservative data are used.

With regard to components whose design is not yet precisely defined or which are not used in French or German plants, reliability data is taken from the EG&G database.

2.1.3. Initiating events

2.1.3.1. General

The initiating events considered are limited to internal events, except for external hazards which can affect the safety of the reactor (i.e. loss of the ultimate heat sink (water intake)).

The initiating events are evaluated from:

- French or international feedback,

- calculations of the failure probability of specific equipment (Loss of cooling systems...), using the component reliability database.

The initiating events studied in the probabilistic evaluation are grouped as follows:

- Loss of primary cooling accident [LOCA],
- Containment bypass,
- Secondary system break (SSB):
    - Breaks on secondary side (steam or feed water) (SLB, FLB),
    - Steam line break and SGTR.
- Steam generator tubes rupture (SGTR),
- Secondary system transients
- Loss of off-site power (LOOP),
    - total loss of off-site power (2h),
    - total loss of off-site power (24h),
    - total loss of long-term off-site power,
    - Common Cause Failure of LH switchboards (CCF-LH).
- Primary system transients:
    - homogeneous dilutions,
    - total loss of RIS/RRA [SIS/RHR] in shutdown states,
    - uncontrolled drop of primary coolant level,
    - loss of RCV pumping.
- Loss of cooling water systems:
    - partial or total loss of cooling chain,
    - loss of ultimate heat sink.
- Transient without automatic reactor shutdown (ATWS),
- Heterogeneous boron dilution.

The application of the break preclusion principle to the main pipework of the reactor cooling system leads to a very low probability of a severe break occurring in its systems (see Section C.4.2.3). The probability of the occurrence of single initiating events corresponding to 2A LOCA and 2A SLB accidents is considered sufficiently low not to require consideration in the PSA. The same applies to the breakages of 'unbreakable components' such as the reactor vessel, steam generators and reactor primary coolant pump [RCP].

2.1.3.2. Quantification of initiating events

The quantification method depends essentially on the initiating event group.

- For initiating events already observed:
    - o F = n/T : where n is the number of occurrences of the event in the sample studied and T is the observation period of the sample (in reactor-years);
    - o for frequent initiating events (i.e. those observed at least once in French plants), the operational experience of the 1300 MWe PWR level is preferred, possibly increased on a case by case basis by operational experience from French 900MW stations.
- for initiating events not observed in French or international feedback, the frequency may be evaluated in two ways:
    - o The χ^2 method at 50% at two degrees of freedom: The estimator of the frequency is calculated as the upper bound of the unilateral confidence interval at the 50% confidence level. In fact, the estimator value is such that the actual frequency at the same probability could be lower (0.5) or higher. Therefore:

      f = $\frac{\chi^2_{0,5}}{2T} = \frac{0.7}{T}$ where T = period of sample observation (in years×reactor);

    - o By 'expert judgement': based on design studies or other special studies.

      Generally, the systematic use of the χ^2 method at 50% is to be avoided because it leads to a homogenisation of the frequencies of all hypothetical initiating events around two values. This homogenisation conflicts with the PSA objective, which is to give priority to sequences leading to core damage. As far as possible, expert judgement is preferred for initiating events not observed at a nuclear site.
- For the initiating events due to equipment failure: the frequency is calculated from reliability data on equipment considered.

  The reliability data is generally available either in the form of an hourly rate of operational failure (λ, reactor/hour) or in the form of a probability of failure on demand (γ, reactor /request).

  The frequency of the initiating event is thus:

$f = \lambda \times Tm$ or $f = n \times \gamma$

where Tm: length of equipment mission considered in hours/year,

n: number of demands on equipment, per year

2.1.4. Common cause failure

Common cause failures (CCF) are those failures on demand or during operation or during the mission period that could simultaneously affect several components, where the failures are due to the same cause. Common cause failures include failures of the equipment itself due to errors of design, manufacture, installation or utilisation.

CCF concerns groups of identical redundant equipment, operating in comparable conditions.

An identical model is used for various types of component: pumps, valves, diesels, high and medium voltage circuit breakers, sensors etc.

No account is taken of a CCF on a group of identical pieces of equipment in the following cases:

- when certain pieces of equipment do not change state during an accident (e.g.: switchboards). In this case, failures may be detected as disturbances to normal operation. These failures may thus increase the failure rate and an analysis is carried out regarding repair and prevention on the other redundant equipment;

- when several identical components, such as contactors and emergency switchgear, operate under similar conditions. In this case most of the failures will be detected by observation, allowing corrective measures to be carried out.

CCF of identical components is considered when the components belong to the same system and have the same function. At present, CCF of the low-voltage circuit breakers of the ISMP [MHSI] pumps is taken into account in the ISMP [MHSI] modelling. A CCF of the same component belonging to different systems is not considered because these components have different functions, and different test and maintenance regimes. For example CCF of low-voltage circuit breakers of the ISMP and similar equipment on other systems (e.g. ASG [EFWS] pumps) is not considered.

The following deals with the particular case of CCF for back-up batteries

- Specific CCF factors are defined for batteries involved in the temporary re-supply of the electrical distribution switchgear, taking into account pre-accident failures.

- The CCF factors are established by use of international feedback on batteries in groups of 2, 4, 5, 6, 9, and 16 components.

2.2. CONSIDERATION OF THE INSTRUMENTATION AND CONTROL SYSTEM

2.2.1. Introduction

Given the relatively important role played by the instrumentation and control system in the overall core damage frequency, the decision was taken to integrate this system into the PSA model.

This integration was carried out in two stages:

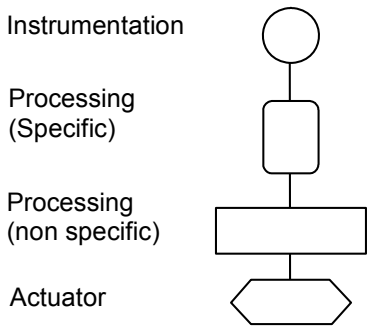
- modelling of the I&C control channels with the 'Compact Failure Model'.
- global integration of the I&C functions in the PSA model.

These two stages are summarised below.

2.2.2. Methodology

The instrumentation and control modelling is referred to as the 'compact failure model'. The modelling is based on the logical breakdown of the I&C automatic missions into large sub-functions.

From this, as shown in the following symbolic representation, each single instrumentation and control channel is broken down into three main parts: an instrumentation part, a specific and non-specific processing part, and an actuator part.



Symbolic representation of an instrumentation and control system

For final integration into the PSA event trees, these symbolic representations of failures are converted into fault trees.

In the fault trees, fixed numerical values for overall unavailability are applied for the instrumentation and processing parts. They depend on the classification and internal architecture and may be used directly in the PSA Boolean modelling.

The numerical values for the actuator parts are obtained from failure rates or actuator unavailability values (mechanical parts, circuit breakers etc.).

2.2.2.1. Instrumentation part

This part is made up of a group of redundant sensors (the term 'sensor' includes the measuring cell, the electronic converter and the transmission connector technology) and of the implementation of the same parameter. The number of sensors in the group depends on the internal redundancy level of the protection system: for example, a redundancy of 2/4 requires four sensors.

2.2.2.2. Processing part

This part is made up of two sub-parts:

- a part specific to a given protection system and its processing logic. This part extends from the acquisition of the parameters (downstream of the sensors) to the generation of the partial instructions (before voting). It includes all the redundant printed circuit boards (hardware and software) required for partial instructions. It takes account of the internal redundancy levels of the system;

- a part common to all the systems and specific to a given programmable logic controller. It takes account of all the components used for the voting processing. It includes, moreover, all the elements, systems and common protocols indispensable to data transmission (for example: the data buses, the exchange protocols, etc). This part also takes includes the common equipment points as well as common cause failures that may be introduced by use of common technology.

2.2.3. Instrumentation and control unavailability values

The overall unavailability values of each part are based on many parameters, reflecting the attention given to the quality of the construction and manufacture of controllers (classification of equipment). The values refer to a single protection system. They are based on expert judgement and are compatible with feedback and reliability studies on the instrumentation-control systems performed by EDF for the PSA 1300 and N4. The values are of the same order of magnitude as values proposed in international standards.

The figures used are the same for E1B, E2 and NC systems. This is based on the assumption that the general quality level of part of a class E2 or NC system dedicated to a function is in the same range as that of an E1B system, from a reliability point of view. If this is not the case, the unavailability values for E2 and NC systems are increased.

2.2.3.1. Instrumentation part

The numerical values for a group of sensors take account of:

- the internal architecture (degree of redundancy, etc.),

- the common cause failure rates, calculated according to the β factor method,

- calibration errors,

- the efficiency of the internal self-tests conducted in the logic part,

- the time interval between the periodic tests, the operating technical specifications and the general quality of the system (reconfiguration etc.).

If a system requires N groups of sensors to function, the risk of unavailability of the group will be counted N times.

2.2.3.2. Specific processing part

The numerical values are standard envelope values taking account of:

- system internal architecture and logic (degree of redundancy, etc.),

- design errors

- independent failure rates and common-cause failures of equipment origin, affecting redundant components (e.g. 4 boards for a redundancy of 4),

- failures due to software packages specially developed for a given system and for a specific requirement. These packages are application software which requires the development of a specific logic (threshold overshoot, taking account of particular operating conditions, use of permissives),

- internal diagnosis self-test frequency,

- human errors in data input.

Note: for the F2 and NC systems used in the safety evaluation, an unavailability of 10^{-3}/demand is used for the specific processing parts, provided design provisions (redundancy, independence in terms of process interruptions caused by the accident) are sufficient. Otherwise, a higher value is adopted.

2.2.3.3. Non-specific processing part

The numerical values used for the unavailability are global values, which dependent essentially on the class of I&C controllers. The global unavailability values allow for:

- common cause failures due to errors in the operating software and data exchanges on networks,

- internal common points in the hardware or software, (data buses, communication protocols common to all boards, etc.),

- common cause failures due to use of the same technology (design, manufacture, etc.).

The proposed values are ten times lower than those used for the specific parts of systems. The reason is as follows:

- hardware and software in non-specific parts are not custom-developed. They have generic characteristics (operating system software, data buses, exchange protocol, etc.),

- due to their function, these components and software are common to all systems. Their failures thus may have critical consequences. Therefore they are subject to strict construction procedures and strict monitoring and checking,

- these components are in extensive use, and can thus be regarded as tried and tested hardware and software items, giving a high level of confidence in their operating dependability.

2.2.4. Integration of the instrumentation and control in the PSA model

2.2.4.1. Scope of study

The global integration of I&C functions in the EPR PSA has been performed for the following I&C functions:

- protection systems: reactor automatic shutdown channels and auxiliary safeguard start-up channels,
- 'risk reduction' channels linked to protection system unavailability: for example ATWS due to mechanical seizure of control rods,
- control actions are not taken into account in the PSA. A Limiting Condition of Operation (LCO) corresponding to the first control rod insertion limit signal (control rod insertion activated by Reactor Power control) is assumed.

The instrumentation and control system missions represented in the model are listed in the following table:

Group of Protection Systems	
1.	Automatic reactor trip (1)
2.	ATWS (mechanical blockage of the rod clusters or failure of the protection system)
3.	Safety Injection System (RIS) [SIS]
4.	Chemical and Volume Control System (RCV) [CVCS]
5.	Extra Boration System (RBS) [EBS]
6.	Start-up and Shutdown System (AAD) [SSS] / Normal supply of steam generators (APA [MFWPS],ARE [MFWS])
7.	Emergency Feedwater System (ASG) [EFWS]
8.	Steam Generator Blowdown System (APG) [SGBS]
9.	Main Steam Bypass to the condenser (GCT) [MSB]
10.	Partial cooling
11.	Main Steam Atmospheric Dump System (VDA)
12.	Main Steam isolation valves (VIV) [MSIV]
13.	Turbine Trip
14.	Reactor Coolant System (RCP) [RCS]
15.	Containment isolation
16.	Emergency Diesel Generator [EDG]
17.	Component Cooling Water System (RRI) [CCWS]
18.	Essential Services Water System (SEC) [ESWS]
19.	Demineralised Water System (SER) [DWS]

(1) Failure of the reactor trip breakers and the seizure of a rod cluster control assembly are considered separately.

Permissive and conditional signals

Unavailability of permissive signals is, in general, not taken into account. The effect is considered to be negligible. A permissive signal is generally representative of a stable plant state (e.g. Nuclear power > 10% of nominal power). This unavailability would be detected by different methods (monitoring systems, operators, etc.) during normal operation. Consequently, the effect of an independent failure of a permissive signal coinciding with a failure of protection signals during a transient is considered negligible.

2.2.4.2. General assumptions linked to I&C integration

Insertion of instrumentation and control in the event trees:

The principle followed is to incorporate the I&C fault trees into the event trees as generic events. This option helps improve the representation of the accident development and the countermeasures taken to mitigate the initial event.

In practice, certain protection signals do not have a global effect on a system, as they are characterised by channels specific to each train: thus each ASG [EFWS] train is activated by a specific protection channel which uses specific measurements from the connected steam generator.

This situation occurs for diesel start-up, the engagement of the reactor coolant pumps, the activation of the DEA [SSSS], etc.., where the instrumentation and control actions are initiated by a specific protection channel for each train. The modelling of the signals as top events would be difficult, due to the combination of numerous events and sequences involved in modelling the various combinations of I&C and mechanical failures. Failure of these protection channels is therefore included in the system fault trees.

In a configuration where the initiating event is studied in states 'A and B', the instrumentation and control signals considered are those valid for state A. If a more detailed model is necessary, this type of event tree is copied and adapted for state B: this is the case for an SGTR in states A and B, for example.

Operator recovery aspects:

For many instrumentation and control mission failures, operator actions may be considered as recovery measures. A full analysis is performed, in order to ensure that possible recovery actions by the operating team has been incorporated, taking into account the detailed design of the main control room.

However, recovery actions by the operating team may only be included if:

- the operator has enough time to diagnose the problem and carry out the appropriate actions,
- a diagnosis is performed using data of which is sufficiently diverse from that used to generate the automatic instrumentation and control actions that the manual action replaces,
- no total dependence on a preceding operator action is revealed.

Specific probabilistic assumptions:

- the processing part specific to a channel is generally considered as being the same for channels of the same class (e.g. pressuriser pressure very low for RIS [SIS] actuation and pressuriser pressure low for reactor trip) which use same control part but not the same threshold.
- the same specific part failure is used for analogous channels related to a specific train, e.g. for steam generators or reactor coolant pumps.

2.3. HUMAN RELIABILITY ANALYSIS

2.3.1. Introduction

In normal operation, human errors may contribute to an accident. In accident situations, both safeguard systems and human actions are necessary to bring the facility back into a state of 'control'. In normal or accident situations, the study of pre-accident and post-accident human errors is ensured by the Human Reliability Analysis (HRA).

2.3.2. Methodology

2.3.2.1. General

Incorporation of human factors in the PSA consists of:

- listing all the potential and significant human errors capable of causing an accident or causing the failure of a safeguard mission after the occurrence of an initiating event,
- assigning a probability to these human errors;
- in case of "pre-accident errors", reintroducing them as basic events in the fault trees that model the safeguard system missions (e.g. valve left in closed position),
- in case of "post-accident errors", reintroducing them in point-value form as leading (top) events in the accident sequences (e.g. failure of implementation of feed and bleed).

The method for deriving Human Error Probabilities (HEPs) is based on the work of Swain and, essentially, on the simplified model for quantification of post-accident errors (the 'screening model') termed the 'ASEP HRA Procedure' method [ASEP: Accident Sequence Evaluation Programme].

As human errors before or during an accident can be recovered in certain circumstances, the simplified model has been adapted to allow for error recovery factors.

2.3.2.2. Pre-accident human errors

Pre-accident errors are made those during normal operation. As they affect safeguard systems, they may contribute to an accident or hinder its recovery.

These errors may occur in any case where an actuator is manually adjusted. In safety systems, such manual adjustments are performed, in particular, during periodic testing and maintenance. For this reason, errors prior to an initiating event are often assimilated with errors made during testing or maintenance, although there is no complete equivalence (e.g. manually operated ASG [EFWS] gate valve left in the closed position).

The probability of such an error is quantified by:

$$\mathbf{P = P_b \times P_{NR}}$$

where :

Pb Basic probability of human error for the pre-accident tasks,

P_{NR} Probability of non-recovery on the basis of favourable recovery factors.

2.3.2.3. Post-accident human errors

These errors fall within the scope of accident management. Post-accident errors include diagnosis errors (e.g. selection of incorrect accident procedure or non-compliance with the correct procedure) and operator errors due to incorrect or late implementation of safeguard actions specified in accident operating procedures.

The probability of such an error is calculated from:

$$P = P_d + (1 - P_d) \times P_a \times P_{NRa}$$

where :

Pd : Probability of incorrect diagnosis,

Pa : Probability of incorrect action following a correct diagnosis,

P_{NRa} : Probability of non-recovery from an incorrect action.

2.3.2.4. Modelling dependency between operator actions

A French approach to modelling dependency between the failure of operator actions is used. It consists of assigning a conditional probability of 0 (no dependency), 0.1 (medium dependency or 1 (total dependency), when two operator missions are modelled in the same accident sequence.

2.4. PREVENTIVE MAINTENANCE

Preventive maintenance is modelled in the PSA using the following assumptions:

The maintenance scenario takes into account the maintenance phases on certain groups of systems.

Phase 1: 28 day duration in state A – Unavailability due to preventive maintenance of an electrical supply train supporting the following systems is assumed: ASG[EFWS]/RRI[CCWS]/RIS[SIS]/SEC[ESWS]/EDG[1].

Phase 2: 14 day duration in state A – Preventive maintenance on the AAD [SSS] system is considered.

Phase 3: 14 day duration in state A – Preventive maintenance on one of the 2 trains of systems RCV[CVCS]/REA[RBWMS] is considered.

Phase 4: 14 day duration in state A – Preventive maintenance on one of the 2 SBO emergency diesels is considered.

Phase 5: 14 day duration in state A – Preventive maintenance on one of the 2 trains of the EVU [CHRS] system is considered.

Phase 6: 150 hours duration in state E – successive preventive maintenance campaigns on one safeguard train is considered for all systems: ASG [EFWS], RRI[CCWS], RIS [SIS], SEC [ESWS] and EDG as well as for the SBO-DG system recognising that the latter will never be in maintenance at the same time as the EDG system (total maintenance time shared between with EDG and SBO-DG systems).

This study is integrated into the PSA model using the following:

- basic events representing loss of trains for maintenance,
- house events that allow the imposition of preventive maintenance globally,
- house events that allow the imposition of preventive maintenance on particular systems for specific studies,
- for each system, a fault tree corresponding to unavailability due to preventive maintenance, (activated if needed),
- a certain number of boundary condition sets covering various combinations of preventive maintenance assumptions.

During the detailed studies phase, the above approach is likely to evolve (e.g. not taking account of phase 3).

[1] Main Emergency Diesel Generators

2.5. GENERAL ASSUMPTIONS IN SYSTEM MODELLING

2.5.1. Methodology

Principles applicable to analysis method the specification of the EPR reliability study are given below.

For constructing the accident scenarios, the missions of the required protection systems, identified by functional analysis, are first modelled.

The modelling of the system mission uses a Boolean method based on fault trees.

A fault tree is developed for each system mission. This allows a qualitative identification of the minimum cut sets leading to failure of the system mission and calculation of the probability of the failure and the corresponding minimum cut sets:

- a cut set represents a combination of equipment failures or human errors leading to an event (such as a top event), or of a sequence or consequence,

- the expression “minimum cut sets” refers to any cut set corresponding to the smallest possible combination of independent equipment failures or human errors leading to the occurrence of an event, sequence or consequence.

2.5.2. System mission times

As a Boolean method is used, the reliability of systems may be uniquely quantified for a single mission time with no possibility of repair, independently of the actual duration of the various missions required.

The EPR PSA model uses a mission time of 24h, in line with standard international practice.

Note: This value is conservative in the case of initiating events that allow a rapid recovery, such as the loss of off-site power [LOOP] for 2 hours, or rapid Anticipated Transient Without Scram (ATWS).

2.5.3. Introduction of PSA support systems

The support systems ensure correct operation of the main systems by providing a power source (electricity, steam, compressed air, etc.) and/or by enabling system operation to be maintained (refrigerated water, ventilation air, lubrication oil, etc.).

Five support systems are considered and modelled:

- electrical sources (high voltage),

- Component Cooling Water System (RRI) [CCWS],

- Essential Services Water System (SEC) [ESWS],

- diversified heat sink for trains 1 and 4 of the ISBP [LHSI] pumps,

- diversified heat sink of the cooling system of a dedicated EVU [CHRS] (and third PTR [FPPS/FPCS] train).

The electrical sources and the RRI [CCWS] and SEC [ESWS] support systems are modelled directly in the fault trees representing the main systems (for example, RRI [CCWS] and SEC [ESWS] pumps and the electrical power supply to the actuators are included in the RIS [SIS] system fault tree).

The CCWS and ESWS systems and the electrical sources have been the subject of detailed reliability analysis to identify the required missions following different initiating events (e.g.: in case of LOOP, total loss of ARE [MFWS], small break LOCA).

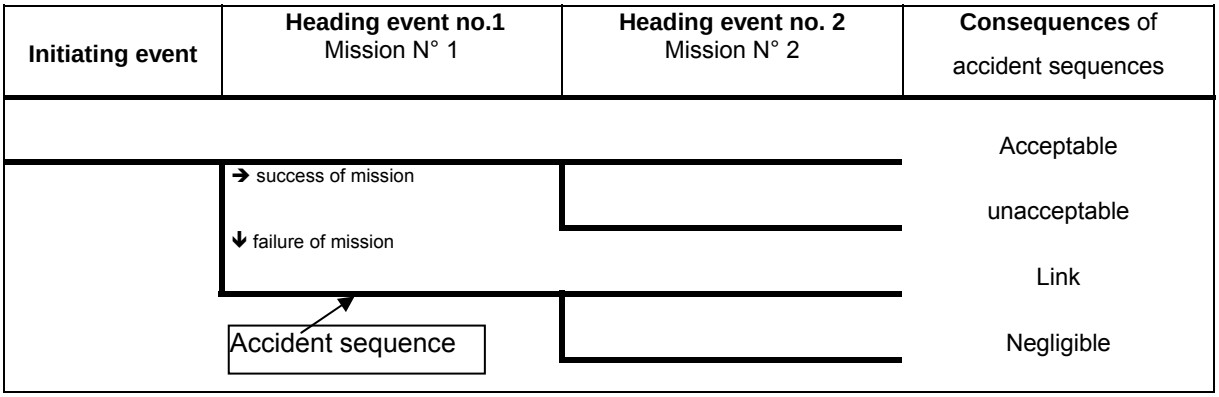
2.6. GENERAL ASSUMPTIONS IN ACCIDENT SEQUENCE MODELLING

2.6.1. Definitions

2.6.1.1. Event trees

An event tree is a decision tree made up of an initiating event and successive events (headings or top events) for success or failure, characterising the PSA sequences.

An accident sequence in an event tree represents an accident scenario. The structure of an event tree comprises all possible accident sequences, i.e. all accident scenarios following a given initiating event.



Example of an event tree

2.6.1.2. Consequences

A consequence represents the endpoint of an event sequence within a given time interval (sequence monitoring time).

For the EPR level 1 PSA, the consequences are of the four following types:

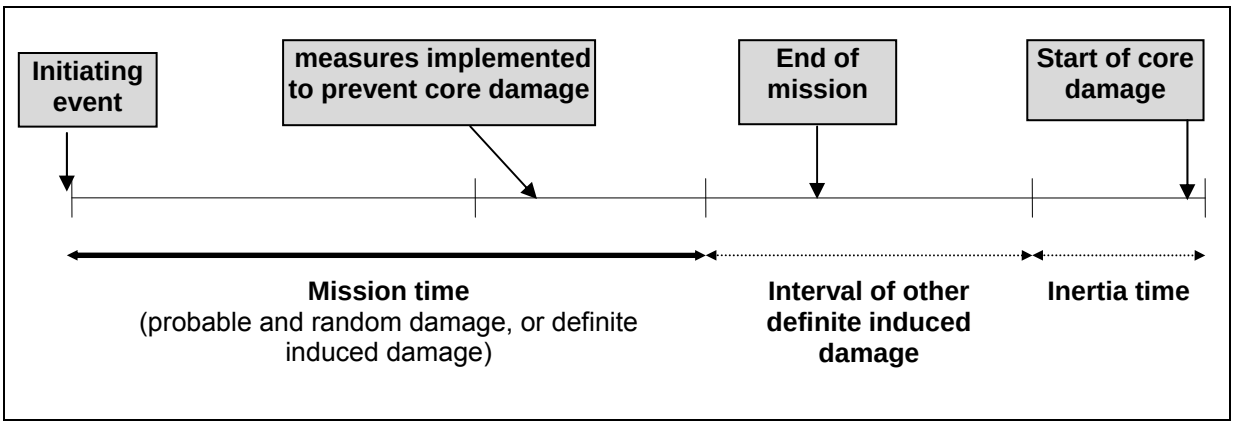
- 'acceptable consequences' indicate that all the system missions and human actions carried out in reponse to the occurrence of an initiating event have ensured that the core damage criteria were not exceeded,
- 'unacceptable consequences' characterise event sequences leading to core damage,
- 'negligible consequences' indicate that the frequency of occurrence of the consequences due to an accident sequences is less than 10^{-12}/ry. This type of consequence is introduced in the PSA for simplification purposes.
- 'link consequences' are referred to when the consequences of an accident sequence are reintroduced into other event tree in the form of an initiating event.

Decoupling criteria are used to define unacceptable consequences

All success criteria and decoupling data are defined at the start of each study.

2.6.1.3. Mission time

A sequence mission time is the elapsed time after the occurrence of the initiating event during which possible failures affecting the PSA mission are considered. In the case of an acceptable sequence, the mission time is simply the time taken to reach the safe state or the shutdown state. This time is limited to 24 hours. For a postulated sequence, it is generally a time that is different from and shorter than the time to reach the start of core damage. It is defined by the moment at which the last main mission ends, i.e. the final safety measures to prevent core damage. The figure below illustrates the various time concepts applied to accident sequences.



Concept of mission time

2.6.2. Modelling of level 1 PSA accident sequences

The EPR project uses an event tree method for modelling accident sequences.

Detailed functional analysis, previously carried out to identify the system missions, is used in the construction of the event trees.

For each initiating event, accident sequences are drawn up, indiacting success or failure of the required missions to the restore safety functions, in the form of a tree structure.

A consequence is then linked to each accident sequence.

In summary, the following elements are necessary to build an event tree:

- initiating event data,
- identification of the required safeguard missions (functional analysis) and their modelling,
- the construction of a tree structure constituting a graphic representation of the accident sequences.

3. RESULTS

3.1. BREAKDOWN OF CORE DAMAGE FREQUENCY INTO INITIATING EVENT GROUPS

3.1.1. Loss of primary coolant accidents (LOCA) group

3.1.1.1. CDF due to LOCA group

The CDF related to the LOCA group may be broken down by initiating events as follows:

- intermediate break LOCA (125 to 830 cm²), States A + B: $6.36\ 10^{-9}$/r.yr
- small break LOCA (45 to 125 cm²), States A + B: $6.72\ 10^{-8}$/r.yr
- very small break LOCA (25 to 50 cm²), States A + B: $2.30\ 10^{-9}$/r.yr
- very, very small break LOCA (2 to 25 cm²), States A + B: $5.10\ 10^{-8}$/r.yr
- very small break LOCA (2 to 5 cm²), States C,D and E: $4.44\ 10^{-10}$/r.yr
- Pressuriser break, States A + B: $9.26\ 10^{-9}$/r.yr

The total core damage frequency of the LOCA group is $1.37\ 10^{-7}$/r.yr

3.1.1.2. Analysis of results

- The 'small break LOCA in states A and B (45-125cm²)' initiating event represents 47% of the CDF of the LOCA group ;
- The 'very small break LOCA in states A and B' initiating event (divided in two parts: 2 – 25cm² and 25 – 45cm²) represent 36% of the CDF of the LOCA group ;
- The 'small break LOCA in states A and B (45-125cm²)' initiating event represents 7% of the CDF of the LOCA group ;
- The 'intermediate break LOCA in states A and B' initiating event represents 5% of the CDF of the LOCA group ;

The major contributions of system missions and operator actions to the risk of unacceptable consequences from LOCA initiating events in all modes are:

- safety injection system and the residual heat removal systems, due to total system loss and common cause failure of pumps for water makeup or resiual heat removal (contributing approximately 72%);
- operator actions linked to secondary cooling control (more precisely with operator the adjustment of set points of partial cooldown, depressurisation via the secondary cooling system and to the activation of the feed and bleed (contributing approximately 65%);
- main steam bypass/ main steam atmospheric dump system / main steam safety relief valves, whose failure results in loss of residual heat removal by the steam generators (contributing approximately 32%);
- instrumentation & control (contributing approximately 15%).

3.1.2. Secondary Side Breaks (SSB) group

3.1.2.1. CDF due to SSB group

The CDF due to Secondary Side Breaks (SSB) may be broken down by initiating event as follows:

- large MSLB outside containment, downstream from the mean steam isolation valves: $1.57\ 10^{-8}$/r.yr
- small break of the secondary side, not isolatable, outside containment (MSLB or FWLB): $3.23\ 10^{-9}$/r.yr
- MSLB with SGTR:
  - main steam atmospheric dump valves kept open (VDA) + two tube SGTR: $1.70\ 10^{-9}$/r.yr
  - large MSLB outside containment, downstream from the main steam isolation valves + two tube SGTR:: $6.48\ 10^{-10}$/r.yr
  - small MSLB outside containment, upstream from the main steam isolation valves + two tube SGTR: $3{,}86\ 10^{-9}$/r.yr

The total core damage frequency due to the SSB group is $2.53\ 10^{-8}$/r.yr

3.1.2.2. Analysis of results

For the MSLB or FWLB sub-group:

- the CDF due to breaks of the secondary side is 1.9 10^{-8}/r.yr (small+large break), of which 60% is due to large MSLB outside containment downstream of the main steam isolation valve.
- the 'outside containment secondary side non-isolatable small break' initiating event contributes 13% of the risk from this event group.
- the dominant small SSB sequences correspond to failure of steam generator heat removal (failure of emergency water supply system/steam dump valves on intact SG following steam isolation) and to the failure of the manual feed and bleed actuation to transfer residual heat into the containment.

3.1.3. "Steam generator tube rupture" group (SGTR)

3.1.3.1. CDF due to SGTR group

The CDF due to the SGTR group is broken down by initiating event as follows:

- SGTR - one tube failure at power: 7.08 10^{-11}/r.yr
- SGTR - two tube failures at power: 2.90 10^{-10}/r.yr
- Small SGTR at power: 1.05 10^{-09}/r.yr

The core damage frequency due to the SGTR group is 1.41 10^{-09}/r.yr

3.1.3.2. Analysis of results

Small steam generator tubes ruptures at power contribute approximately 70% of the CDF due to the SGTR group.

The MSSS and VDA steam discharge systems for cooling of the primary (particularly in the case of non-isolation of the affected steam generator) are present in approximately 52% of the cut sets.

To prevent SG overfill, the design inclues an automatic signal to trip the CVCS pumps. Credit is taken of the automatic F1A signal that isolates the charging line when a very high SG level is reached, if partial cooling is terminated.

3.1.4. "Secondary system transient" group

3.1.4.1. CDF due to group

The transient studied for this group is the total loss of feed water to the steam generators in states A and B.

The core damage frequency due to the "secondary side transients" group is 1.10 10^{-7}/r.yr

3.1.4.2. Analysis of results

Feed and bleed actuation (operator action contribution approximately 93%) is modelled on total loss of normal SG feed water followed by loss of the emergency SG feed water system (essentially due to a common mode on the four trains or to a failure of the I&C (contribution approximately 60%)).

3.1.5. "Total loss of offsite power" group (LOOP)

3.1.5.1. CDF due to LOOP group

Thia group involves accident sequences initiated by a loss of offsite power and common cause failure on the LH switchboards. Five initiating events are analysed:

LOOP for 2 hours in states A and B:	1.68 10^{-09}/r.yr
LOOP for 24 hours in states A and B:	5.95 10^{-08}/r.yr
LOOP for 2 hours in shutdown state:	1.99 10^{-11}/r.yr
LOOP for 24 hours during a shutdown:	1.52 10^{-08}/r.yr
Common cause failure (CCF) on LH switchboard	5.12 10^{-09}/r.yr

The core damage frequency following total loss of offsite power is 8.15 10^{-8}/r.yr

3.1.5.2. Analysis of results

The sequences arsing from the ' total loss of offsite power for 24 hours, at power' initiating event represent approximately 73% of the CDF of this group. These sequences are characterised by either loss of residual heat removal by the secondary and the primary systems in the containment, failure of feed and bleed (safety injection trains and the volumetric and primary system chemical control system unavailable to provide water supply), or by unavailability of the containment heat removal system.

The most significant sequence, contributing 33% of the group CDF, corresponds to a total loss of offsite power for 24 hours at power with unavailability of medium-pressure safety injection systems or of the low-pressure safety injection systems (due to a common cause failure of the main diesel generators).

3.1.6. "Primary system transient" group

3.1.6.1. CDF due to group

The CDF due to the group is broken down by initiating event as follows (regrouped into sub-groups):

- homogeneous boron dilution at power: 2.83 10^{-9}/r.yr
- homogeneous boron dilution in shutdown: 7.67 10^{-9}/r.yr
- total loss of ISBP[LHSI]/RRA[RHR] in shutdown: 1.92 10^{-10}/r.yr
- uncontrolled drop in Primary level in shutdown: 5.01 10^{-9}/r.yr

- total loss of RCV [CVCS] pumps at power: $9.81\ 10^{-9}$/r.yr

The core damage frequency due to the primary system transients group is $2.55\ 10^{-8}$/r.yr

There are two types of boron dilution:

- homogeneous boron dilution (boron concentration roughly the same throughout the primary system);
- heterogeneous boron dilution (water plugs with a low boron concentration are formed in certain parts of the primary system, while the boron concentration in the rest of the primary system is unchanged).

Sub-section R.1.3.9 describes the scenarios studied involving external heterogeneous dilution.

3.1.6.2. Analysis of results

3.1.6.2.1. Homogeneous dilution

Homogeneous boron dilution during shutdown contributes approximately 30% of the CDF from all primary system transients, and approximately 73% of the homogeneous boron dilution CDF in all plant states.

The major contributions to the CDF for this type of initiating event are linked to:

- operator actions (approximately 100% of the cut sets): failure to manually isolate the dilution,
- instrumentation and control (approximately 70% of the cut sets): failure of automatic isolation of the boron and water makeup systems, failure of automatic RCV [CVCS] isolation systems, failure of the changeover by the RCV [CVCS] of boration of the IRWST suction.

3.1.6.2.2. Total loss of ISBP [LHSI] / RRA [RHR]

It should be noted that in the Ca mode, the 4 ISBP[LHSI]/RRA[RHR] trains are lost whereas in the Cb and D modes only 3 ISBP[LHSI]/RRA[RHR] trains are lost.

The major risk due to this type of transient arises from events in state Ca and are mainly due to:

- the containment heat removal system, necessary for removal of residual heat from the containment during feed and bleed operation (approximately 60% of the cut sets) ;
- the ASG/APG [EFWS/SGBS] systems necessary for removal of the residual heat from the RCS via the secondary side (approximately 15% of the cut sets),
- the I&C (approximately 50 % of the cut sets):
- operator actions (approximately 30 % of the cut sets):

3.1.6.2.3. Uncontrolled drop of primary coolant level

The greatest contribution to the CDF (99%) arises in the Cb state because of the high initiating event probablity in this state.

The main minimum cut set (98%) involves failure of manual closing of the RCV [CVCS] valve, failure of the common logic part of the 'low level, < min 1 PTAEE [LOOP]' signal and failure of the operator to activate an ISBP [LHSI] train in RRA[RHR] mode at 30 minutes.

Specific studies have shown that the ISBP[LHSI]/RRA[RHR] pumps may be kept in operation in the event of a drop in level (adjustment of the support signal threshold for the ISMP [MHSI]).

3.1.6.2.4. Total loss of RCV [CVCS] pumps

The major sequences for this type of initiating event arise from small breaks occurring after total loss of the RCV [CVCS] pumps at power.

The system and operator failures making the main contributions to core damage frequency are:

- I&C (75% of the cut sets), linked mainly to activation of the safety injection signal ensuring the primary cooling water supply,
- operator actions (75% of the cut sets), with a large contribution arising from failure to trip of the reactor coolant pumps within 10 minutes.

3.1.7. "Loss of cooling systems" (LOCC) and " Loss of ultimate heat sink" (LUHS).

3.1.7.1. CDF due to group

The CDF due to the group is broken down by initiating event as follows:

- Partial loss of CCWS/ESWS in states A and B: $3.86\ 10^{-8}$/r.yr
- Total loss of CCWS/ESWS in shutdown states: $1.50\ 10^{-8}$/r.yr
- Total loss of ultimate heat sink in states A and B: $4.31\ 10^{-8}$/r.yr
- Total loss of ultimate heat sink in shutdown states $2.53\ 10^{-9}$/r.yr

The core damage frequency for the "Loss of cooling systems" group (LOCC) and "Loss of ultimate heat sink" group (LUHS) is $9.92\ 10^{-8}$/r.yr

3.1.7.2. Analysis of Results

The major contribution to the CDF due to loss of ultimate heat sink initiating events arises from instrumentation & control actions (35% of the cut sets).

The major contributions to the CDF due to total or partial loss of the component cooling water system or the essential service water system arise from:

- operator actions, present in 60% of the cut sets; examples are failure to start up feed and bleed before 90 minutes, and failure of operator to trip the reactor coolant pumps within 10 minutes;

- instrumentation & control (40% of the cut sets).

3.1.8. "Anticipated Transient without Scram" (ATWS)

3.1.8.1. CDF due to group

The CDF due to this group may be broken down by initiating event type as follows:

Partial or total loss of the normal water feed system with failure of the Automatic Reactor Trip	4.2 10^{-8}/r.yr
Transient of loss of secondary load with failure of Automatic Reactor Trip	3.74 10^{-9}/r.yr
Transient of steam overflow with failure of Automatic Reactor Trip	1.45 10^{-8}/r.yr
Loss of primary system pump with failure of Automatic Reactor Trip	2.99 10^{-8}/r.yr
Loss of main electrical network with failure of Automatic Reactor Trip	6.84 10^{-9}/r.yr
Primary transients with failure of Automatic Reactor Trip	1.99 10^{-08}/r.yr
Reactivity transients linked to control rods with failure of Automatic Reactor Trip	4.89 10^{-9}/r.yr
LOCA with failure of Automatic Reactor Trip	1.98 10^{-9}/r.yr
SGTR with failure of Automatic Reactor Trip	3.11 10^{-11}/r.yr

The core damage frequency for the ATWS group is 1.24 10^{-7}/r.yr

3.1.8.2. Analysis of results

The three major contributions to the CDF for the ATWS group are the following:

- steam overflow transients with failure of automatic reactor trip (mechanical seizure of at least 3 shutdown rod clusters),
- loss of a reactor coolant pump with failure of automatic reactor trip, representing approximately 25% of the risk,
- partial or total loss of the main feed water system with failure of automatic reactor trip, representing approximately 33% of the risk

The major risk from this type of transient arises from failure of the emergency SG feed water system to remove the residual heat via the secondary side (approximately 50% of the cut sets).

Failure of the I&C equipment generating the various automatic reactor trip signals activated by the steam generator level is responsible for a major contribution to the CDF (approximately 44% of the cut sets).

3.1.9. External heterogeneous boron dilution

3.1.9.1. Scope of study

Boron dilution initiating events may be divided into two groups:

- homogeneous boron dilution: these are progressive events in which the boron concentration of the primary coolant remains homogeneous;

- external heterogeneous boron dilution: these events result from the formation of a unborated water plug flowing towards the core, after start up of a reactor coolant pump,

The objective of 'practical elimination' of the rapid reactivity injection accidents requires a detailed study of each external heterogeneous dilution scenario, taking into consideration all the lines of defence for each scenario.

The analysis is performed in three steps:

- first step: determination of the critical size of the plug of unborated water on the basis of thermal-hydraulic and nuclear considerations which should be avoided in order to prevent all possibility of transient criticality which might threaten the core integrity ;

- second step: all the potential sequences which can lead to transfer of an unborated water plug exceeding the critical size into the core are examined in detail and all methods must be defined to achieve practical elimination of all such sequences (see Chapter S.2.4);

- third step: a probability risk analysis is carried out to verify that the proposed technical solutionsare sufficient to meet the objective of practical elimination.

3.1.9.2. Events which might lead to an external heterogeneous dilution

3.1.9.2.1. Characterisation

External heterogeneous dilution events are characterised by:

- the formation of an unborated water plug of a critical size in the primary system. This could be due to an operational anomaly in a connected system, or an operator error,

- the flow of the plug towards and through the core.

3.1.9.2.2. General assumptions

The dilution is heterogeneous if unborated water plugs with a low boron concentration are formed in certain parts of the primary system, while the boron concentration in the rest of the primary system is unchanged.

A unborated water plug may form solely in the absence of a forced flow in the primary. The plug is propelled towards the core upon restarting of the reactor coolant pumps.

The heterogeneous dilution scenarios can lead to the formation of an unborated water plug greater than the critical size in a loop of the primary system where homogenisation of the fluid is not guaranteed.

The formation of a non critical plug causes a decrease in the boron concentration with no consequence for the integrity of the fuel.

The analysis carried out considers a critical plug size of 4 m³, which could lead to a local re-criticality in the core, impacting on the fuel integrity.

No analysis is thus made of scenarios that:

- involve restarting of one or more reactor coolant pumps when an unborated water plug is below the critical size,
- involve the formation of a unborated water plug less than the critical size,
- are only likely to take place in state F, in which the core is entirely unloaded.

3.1.9.3. Methods of prevention

3.1.9.3.1. General

'Practical elimination' of the external heterogeneous dilution scenarios is based on the following design provisions:

- RCV [CVCS] charging lines: implementation of an automatic switchover of the suction of the charging pumps of the CVCS to the IRWST,
- technical requirements on the heat exchangers cooled by the RRI [CCWS] system.

3.1.9.3.2. Countermeasures in respect of the external heterogeneous dilution initiating events

All possible scenarios likely to lead to external heterogeneous dilutions are examined.

For all scenarios which may lead to the formation of water plugs larger than the critical size of 4 m³, special provisions have been introduced:

- either for their elimination,
- or to significantly reduce the probability of their formation.

The major provision is the isolation (classed F1A) of the RCV [CVCS] suction line of the volumetric control tank on the basis of boron meters connected and installed downstream of the RCV [CVCS] charging pumps. This function was introduced to significantly reduce the probability of the most likely dilution scenarios leading to formation of an unborated water plug (malfunction of the RCV [CVCS] support or operator errors).

3.1.9.4. Summary of results

3.1.9.4.1. Description of major scenarios

(a) Dilution from RCV [CVCS]

<u>S1 Operator error on adjustment of set point of REA [RBWMS] boron concentration</u>

The reactor coolant pumps are stopped following a total loss of offsite power that occurs whilst at power. The adjustment of the boron concentration in the primary circuit or the makeup at the RCV [CVCS] tank is carried out by the operator with an inadequate concentration of boron. The plug thus formed is propelled towards the core by the charging pumps. In addition, the plugs are generated in each reactor coolant pump through injection at seal no.1 and on the cold legs no.2 and no.4, at the level of the RCV [CVCS] nozzles situated downstream of the reactor coolant pumps. The plugs will be propelled towards the core upon restarting of the reactor coolant pumps.

S2: Malfunction of the control system of the REA [RBWMS]

Following a total loss of the external electrical supply under power or in state C during the reactor restart phase, the reactor coolant pumps are stopped, the automatic control of the injected flow (mixture of water and boric acid at 7000 ppm) fails because of a malfunction of a control valve or of the associated I&C.

The operator does not stop the dilution before the formation of a critical plug.

The plug thus formed is propelled towards the core by the charging pumps; further, the plugs are generated in each reactor coolant pump through injection in seal no.1 and on the cold legs no.2 and no.4. The plugs will be propelled towards the core at restart of the reactor coolant pumps.

S3: Wrong boron concentration in the REA [RBWMS] tank.

The boron concentration of the REA tank is less than required after the following operations:

- an automatic makeup of an inadequate concentration by the boric acid evaporator,
- a manual makeup of an inadequate concentration of the batching tank (TEP) [CSTS],
- an incomplete drainage of the REA tank before its filling or after maintenance operations.

A incorrect makeup during the intermediate phase or on cold shutdown may cause the occurrence of a plug in the primary system. The plugs are generated in each reactor coolant pump through injection at seal no.1 and on the cold legs no.2 and no.4.The plugs will be propelled towards the core upon restarting of the reactor coolant pumps.

S4 Tube rupture in an exchanger

The primary pressure drops to less than the RRI [CCWS] pressure, and a leak is detected on a heat exchanger. During depressurisation, unborated water in the RRI [CCWS] enters the primary system. Plugs are generated in each reactor coolant pump through injection at seal no.1 and on the cold legs no.2 and no.4. The plugs will be propelled towards the core upon restarting of the reactor coolant pumps. A plug may also form in the crossover leg at the suction point of the letdown line (case where the leak goes through the letdown line in the opposite direction).

S9 Non-compliance with procedures associated with commissioning of a demineraliser

Scenarios considered relate to the following initiating events:

- when replacing the resins in the demineralisers, the demineralisers must not be activated during the phase preceding the start of the first reactor coolant pump. If this requiremnt is is not followed, the resins are not saturated in boron.

- a demineraliser is isolated during at-power operation, and contains a low boron concentration when it is reconnected to the RCV [CVCS] without being previous drained and with no diversion of liquid to the primary system. The water discharged into the primary may generate a plug in each reactor coolant pump via injection in seal no.1 and in cold legs no.2 and no.4.

S11 Tube rupture (RRI [CCWS] leak) in the condenser, gas cooler or the TEG [GWPS] gasification unit

A leaking heat exchanger tube will result in the transfer of low-boron concentration water to the reactor coolant side of the the degasser. When the degasser is operating, homogenisation of the primary fluid may not be achieved.

Unborated water is thus injected, and plugs are generated in each reactor coolant pump via injection at seal no.1 and in cold legs no.2 and no.4. The plugs may be propelled towards the core upon restart of the reactor coolant pumps.

S16: Residual low boron concentration water in the RCV [CVCS] system after maintenance

After maintenance operations or replacement of components on the RCV [CVCS] system, there is a risk of dilution if the boron concentration in the water used is too low when the system is isolated. The water may be injected in the primary system upon restarting of the reactor coolant pumps. A plug is generated in each reactor coolant pump through injection at seal no.1 and in cold legs no.2 and no. 4.

(b) Dilution from the RIS/RRA

S18: Failure of the RRA pump

The pumps are designed with mechanical seals and hence cooling by the RRI [CCWS] is necessary. Failure of this cooling may lead to a leakage in an ISBP[LHSI]/RRA[RHR] pump when the RRA[RHR] is not connected. If there is a leak, unborated water from the RRI [CCWS] may enter an RIS/RRA train.

S23: Residual low boron concentration water in the RCV [CVCS] system after maintenance

After maintenance operations or replacement of components on the RIS [SIS] system, there is a risk of dilution if the boron concentration in the water used is too low when the system is isolated. This water may remain in the system, and if the ISBP [LHSI] pumps are put into service when there is no circulation, a water plug may be injected via the charging line.

(c) Dilution from the RIS [SIS] accumulators

S30: Residual unborated water in the accumulators after maintenance

After maintenance operations or component replacement, if an accumulator discharges inadvertently following an accident or in a test when the reactor coolant pumps are stopped, a plug may form in a cold leg.

(d) Dilution from the RRI

S39: Rupture of thermal barrier

The primary pressure drops below that of the RRI [CCWS]. A leak (or a non-detected leak) appears through the thermal barrier on a reactor coolant pump. During depressurisation, the RRI [CCWS] unborated water enters the primary system and a plug forms.

(e) Dilution from the environment (opening of reactor coolant system)

S44: Residual low boron concentration water in the RCV [CVCS] system after maintenance

After maintenance operations or replacement of system components, there is a risk of dilution of boron concentration when the system is isolated. A plug may thus be injected via the charging line.

(f) Dilution from the RCV [CVCS] followed by a LOOP

S100: LOOP during normal dilution operations

Following loss of circulation caused by the reactor coolant pumps stopping as the result of a LOOP, residual heat is insufficient to ensure homogenisation of the primary liquid. A plug thus formed may be propelled towards the core by the charging pumps; further, plugs may be generated in each reactor coolant pump through injection via seal no.1 and on the cold legs no.2 and no.4. The plugs could be propelled towards the core on restart of the reactor coolant pumps.

Results

The analysis of the different scenarios leads to a calulated frequency of the formation of an unborated or low boron concentration water plug of a size greater than 4m,³ of 5.20 10^{-09} /r.yr. This frequency is low enough for heterogeneous dilution scenarios to considered the as ‘practically eliminated’.

The various conservative assumptions considered (size of plug, boron concentration, consequences for fuel,…) support the conclusion that the results obtained are acceptable.

3.1.10. Containment bypass

Core damage sequences with containment bypass cover all core damage events where there is direct contact between the primary coolant and the environment.

Scenarios analysed in this section concern LOCAs occurring outside the containment.

3.1.10.1. Scope of study

LOCA sequences leading to containment bypass are associated with breaks on a system connected to the primary system that is partially located outside of the containment: such failures may lead to a loss of primary cooling and an IRWST discharge outside the containment if the break is not isolated.

The study carried out considers the frequency of initiating events leading to a break, and the possible failure of existing barriers or safety measures, leading to risk of a containment bypass.

Breaks outside the containment that are within the charging flow rate capability of the RCV [CVCS] are not considered in the evaluation. Thus only breaks corresponding to leakage rates greater than 36 t/h are considered, taking into account the possibility that an RCV [CCVS] pump may be unavailable for maintenance.

The initiating events analysed and quantified involve the RCV [CVCS], RIS [SIS], RBS [EBS], REN [NSS], RPE [NVDS], EVU [CHRS] systems, the PTR [FPCS] tank, and the RRI [CCWS] system via the reactor coolant pump thermal barriers.

The following bypass scenarios are not analysed in this section (see Section S.2.4 and S.3):

- SGTR + MSLB,
- SGTR with safety relief valve or VDA valves stuck open,
- scenarios induced by severe accident sequences.

3.1.10.2. LOCA leading to a containment bypass via the RCV [CVCS] system

3.1.10.2.1. States considered

The initiating events studied are analysed in states A to Ca. In states Cb to E, the primary pressure is equal to approximately 1 bar and hence there is no risk of a LOCA leading to a containment bypass in these states.

3.1.10.2.2. Bypass scenarios

RCV 1: Break of one or two tubes of the exchanger HP RCV1101 (1102)EX (states A to Ca)

A break of one or two tubes of the HP exchanger causes a leak in the RCV exchanger towards the RRI [CCWS]. The worst consequence of this leak is an reverse flow of primary coolant into the environment via the letdown line and the RRI [CCWS].

The break may be detected by the following indications and alarms:

- measurement of level in the RRI [CCWS] tank (indication),
- measurement of flow on RRI [CCWS] side (indication),
- measurement of temperature on RRI [CCWS] side (alarm),
- measurement of activity to stop RRI [CCWS] pumps (alarm).

The letdown line is automatically isolated on a low pressuriser level by closure of the RCV [CVCS] 1001 / 1002 VP valves. In case of a failure of automatic control, the operator has sufficient time to isolate the upstream heat exchanger via the RCV [CVCS] 1101 VP valve (alarms and indications mentioned above allow the operator to detect the leak after tube rupture).

The RCV 1 scenario consists of the break of one or two exchanger tubes followed by failure of motorised valves RCV 1001 VP, RCV 1002 VP and RCV 1101 VP to close.

RCV 2: Inadvertent opening of the pressure reducing station RCV 1102 (1202)VP (states A to Ca)

Inadvertent opening of the pressure reducing station is detected by:

- the pressure and the temperature downstream from the pressure reducing station,
- measurement of the pressure level.

A break on the letdown line is detected by:

- the pressure and the temperature on the letdown line,
- setting initiated on the water level in the VCT < min,
- sump level (draining system) > max in the fuel building,
- measurement of the activity in the air extraction duct in the reactor building.

The letdown line is automatically isolated on a low pressuriser level by closing the RCV 1001 / 1002 VP valves. In case of failure of automatic control, the operator has sufficient time to isolate the upstream exchanger via the RCV 1101 VP valve (the alarms and indications mentioned above allow him to detect the leak following the tube break).

The RCV 2 scenario is the spurious opening of the pressure reducing station RCV 1102 VP, followed by failure of isolation of the letdown line by the RCV 1001 VP and RCV 1002 VP valves and failure of isolation of the exchanger via the RCV 1101 VP and RCV 1103 VP valves.

RCV 3 and RCV 4 Break or leakage in the RCV makeup line downstream of the control valve RCV 7002 VP (states A to Ca)

The RCV 3 scenario corresponds to leakage or pipe break in the RCV [CVCS] makeup line downstream of control valve RCV 7002 VP, followed by the failure to close of check valves RCV 7005 VA, RCV 7109, 7108 VA and failure to close of the RCV 7008VP motorised valve.

The RCV 4 scenario corresponds to a break in the RCV makeup line piping, downstream of the RCV 7002 VP control valve followed by the failure of the RCV 2006 VP isolation valve and the failure of the RCP1230/32VP check valves.

For these two scenarios, the leakage/break is detected by:

- a charging pump trip due to a break,
- the sump level (draining system) > max in the fuel building,
- measurement of the activity in the air extraction duct in the reactor building.
- pressure measurement.

RCV 5: Break or leakage in the RCV makeup line upstream of the control valve RCV 7002 VP (states A to Ca)

The RCV 5 scenario corresponds to a break in the RCV makeup line upstream of control valve RCV 7002 VP, followed by the failure to close of check valves RCV 7108 VP and RCV 7109 VP and the failure to close of the RCV 7008VP motorised valve.

The leakage/rupture is detected by:

- charging pumps trip due to a break,
- sump level (draining system) > max in the fuel building,
- measurement of the activity in the air extraction duct in the reactor building.

RCV 6: Break upstream of control valve RCV 7002 VP (states A to Ca)

The RCV 6 scenario corresponds to a break upstream of the RCV 7002 VP control valve, followed by the failure to close of the RCV 2006 VA, RCP 1230 and 1232 VP check valves.

The associated consequence is a reverse flow via the makeup line.

3.1.10.3. LOCA leading to a containment bypass on the RIS [SIS] system

3.1.10.3.1. States considered

The initiating events studied are analysed in states A and B.

For the MHSI lines, the primary pressure is equal to approximately 1 bar: hence there are no risk of LOCA leading to a containment bypass in states Cb to E.

3.1.10.3.2. Bypass scenarios

RIS 1 Internal leakage of the isolation check valve RIS1560VP (or of the RIS1510VP motorised valve ((states A and B)

The worst consequence is a reverse flow towards the MHSI lines.

The RIS 1 scenario corresponds to internal leakage of the RIS 1560 VP isolation check valve, followed by the internal failure of the RIS 1540 VP check valve and a failure to close of the RIS 1645 VA check valve.

The internal leakage is detected by:

- measurement of the pressure between the isolation valves on the cold leg of the RIS [SIS] (indication – alarm),
- measurement of the temperature between the isolation valves on the cold leg of the RIS [SIS] (indication – alarm),

If the first check valve develops a leak, it is estimated that the time necessary for the operator to depressurise and cool the reactor before the internal leakage of the second check valve and the failure to close of the RIS 1645 VA valve is sufficient to allow detection of the leak in the first device (the operator being warned by the alarms mentioned above).

RIS 2 Actuation of the ISMP [MHSI] (states A to Ca)

The RIS 2 scenario corresponds to the actuation of the MHSI followed by MHSI pump trip combined with failure of the isolation check valves RIS 1560 VP, RIS 1540 VP and RIS 1645 VA.

RIS 3 Internal leakage of isolation check valve RIS 1560 VP or the RIS 1510 VP motorised valve (states A and B)

The RIS 3 scenario corresponds to internal leakage of the RIS 1560 VP isolation check valve, followed by the internal failure of the RIS 1520 VP check valve and the failure to close of the RIS 1625 VA check valve.

The internal leakage is detected by:

- measurement of the pressure between the isolation valves on the cold leg of the SIS (indication – alarm),
- measurement of the temperature between the isolation valves on the cold leg of the SIS (indication – alarm),

If the first check valve develops a leak, it is estimated that the operator has sufficient time to detect the leak (following receipt of the alarms mentioned above) and to depressurise and cool the reactor before the occurrence of internal leakage of the second check valve and the failure to close of the RIS 1645 VA valve.

The ISBP [LHSI] pump is not in operation, a reverse flow from the cold leg through the pumps may cause a break on the ISBP [LHSI] line.

RIS 4 Actuation of the ISMP [MHSI] followed by an internal failure of the RIS 1520 VP check valve (states A to E)

The RIS 4 scenario corresponds to an actuation of the ISMP [MHSI] followed by the internal failure of the RIS 1520 VP check valve which separates the ISMP [MHSI] and ISBP [LHSI] lines, and to the failure of the RIS 1625 VP valve.

RIS 5 RIS 1510 VP (or RIS 1560 VP) isolation valve left open or develops internal leak (states A and B)

The RIS 5 scenario corresponds to a RIS 1510 VP valve left open or developing an internal leak followed by the two RIS 1515 VP and RIS 1615 VP motorised valves being left open or developing an internal leak.

The leaking or left open motorised valve is detected by:

- a positioning alarm on the valve,

- the following alarms activated after failure of the valves:
    - o high pressure at the SIS/RHR (RIS 1510 VP and RIS 1515 VP) isolation valves,
    - o high pressure at the RIS 1560 VP and RIS 1520 VP) isolation valves,
    - o low level in the accumulator of the train concerned,
    - o low pressure in the accumulator of the train concerned,

RIS 6 Break in the hot leg injection line upstream of the RIS 1615 VP and RIS 3121 VA (states A and B)

The RIS 6 scenario corresponds to a break in the hot leg injection line upstream of the RIS 3121 VA combined with the three valves RIS 1510 VP, RIS 1560 VP and RIS 1515 VP being left open or developing an internal leak.

The motorised valve being left open is detected by a positioning alarm.

Failure of the RIS 1510 VP valve is detected by a high pressure alarm between the RRA [RHR] isolation valves (RIS 1510 VP and RIS 1515 VP) and the isolation gate valves (RIS 1560 VP and RIS 1520/40 VP).

3.1.10.3.3. Break on LHSI/RHR outside the containment in shutdown states

The CDF for the sequences “break in ISBP/RRA [LHSI/RHR] outside the containment” are allocated to the different initiating events as follows:

- Very small external break (< 70 t/h - (DN25 or 5cm²) on the ISBP/RRA in the states C to E: $2.41\ 10^{-10}$/r.yr
- Small external break (> 70 t/h – DN50 or 20cm² and breaks of a diameter equal to DN250 (size of LHSI/RHR lines) on the ISBP/RRA in states C to E: $5.83\ 10^{-11}$/r.yr
- Rupture of two tubes on the SIS/RHR heat exchanger in state C: $6.00\ 10^{-11}$/r.yr

The total core damage frequency due to these sequences is $3.53\ 10^{-10}$/r.yr

Analysis of results:

- sequences linked to a very small break or leakage outside the containment on the ISBP/RRA [LHSI/RHR] represent approximately 66% of the CDF of this sequence group.
- sequences linked to a small break or leakage outside the containment on the ISBP/RRA [LHSI/RHR] represent approximately 17% of the CDF of this sequence group.
- sequences linked to a tube rupture on the RIS/RRA [LHSI/RHR] exchanger represent approximately 17% of the CDF of this sequence group.

- Previously, the dominant sequences involving a break outside the containment on an ISBP/RRA [LHSI/RHR] train, leading to core damage, were mainly due to mechanical failures of the isolation valve of the affected train. ISBP/RRA [LHSI/RHR] design developments have resulted a reduction in the frequency of these scenarios. The isolation is performed by two diverse RRA [RHR] valves in series.

3.1.10.4. LOCA leading to a containment bypass via the RBS [EBS] system

3.1.10.4.1. States considered

The initiating events are analysed in the states A to E. In normal operation, the pumps are at rest.

3.1.10.4.2. Bypass scenarios

RIS 1: Internal leak of RIS 1560 VP check valve (states A to E)

The RBS 1 scenario corresponds to an internal leak of the RIS 1560 VP check valve (or the RIS 1510 VP motorised valve), followed by the spurious opening of RBS 7115 VA (or this valve being left open) and failure to close of the RBS 7107 check valve and the two ball lift check valves of the RBS pumps.

The internal leakage of the RIS 1510 VP check valve is detected by a high pressure alarm between the RHR isolation valves, RIS 1510 VP and RIS 1515 VP, and a high pressure alarm between the isolation valves, RIS 1560 VP and RIS 1520/40 VP.

If the RIS 3112 VA fails, the following alarms:

- high sump level (draining system) in the fuel building,
- measurement of activity in the air extraction duct of the reactor building,

allow the operator to detect the failure and thus prompt him to carry out necessary reactor depressurisation and cooling operations.

RBS 2: Internal leak of check valve RIS 1560 VP or RIS 1510 VP (states A to E)

The RBS 2 scenario corresponds to the internal leak of the check valve RIS 1560 VP (or RPS 1510 VP) followed by the spurious opening of RBS 7115 VA (or this valve being left open) and the closing failure of the RBS 7107 VA check valve.

The reverse flow thus created causes a break in the RBS [EBS] piping upstream of the pump.

The break is detected by a measurement of the activity in the air extraction duct in the reactor building.

The internal leak of the RIS 3112 VA check valve is detected by:

- a high pressure between the RRA isolation gate valves,

- a measurement of the pressure between the isolation valves on the RIS cold leg.

In the case of a failure of the isolation valves, the break is detected by:

- a high sump level (draining system) in the fuel building,
- a measurement of the activity in the air extraction duct in the reactor building.

RBS 3 and RBS 4: Failure during operation of the RBS [EBS] (states A to E)

The RBS 3 and RBS 4 scenarios correspond to the actuation or the spurious operation of the RBS followed by failure to close of the check valves: RIS 1560 VP, RBS 7115 VA and RBS 7107 VA causing a break in the RBS [EBS] piping.

The break is detected by:

- a high sump level (draining system) in the fuel building,
- measurement of the activity in the air extraction duct in the reactor building.

3.1.10.5. LOCA leading to a containment bypass via the RRI [CCWS] system

3.1.10.5.1. States considered

The states considered are state A and state B.

3.1.10.5.2. Bypass scenarios

RRI 1: Tube break downstream from the thermal barrier

The RRI 1 scenario corresponds to a tube break downstream of the thermal barrier followed by an incorrect position of the RCP 1215 VN control valve and the failure to close of the RCP 1218 VN valve. The break is detected by:

- pressure measurement of pressure upstream of the thermal barrier side of the RRI,
- flow measurement downstream from the thermal barrier side of the RRI,
- measurement of level in the RRI tank,
- measurement of activity.

RRI 2: Tube break upstream of the thermal barrier

The RRI 2 scenario corresponds to a tube break upstream of the thermal barrier followed by failure to close of valves RCP 1211 VN and RCP 1210 VN and the failure to open of the RRI 5510 VN/6510 VN valves.

The break is detected by the signals mentioned above for the RRI 1 scenario.

3.1.10.6. LOCA leading to a containment bypass via the EVU [CHRS] system

3.1.10.6.1. States considered

LOCAs leading to a containment bypass via the EVU [CHRS] system are considered in all states.

3.1.10.6.2. Bypass scenarios

EVU 2 and EVU 3: actuation of the EVU [CHRS] during an accident (states A to E)

The EVU 2 and EVU 3 scenarios correspond to accident sequences necessitating use of the EVU [CHRS] followed by a pipe break on the main system upstream of the first isolation valve and failure to close of the RIS 1009 VA motorised valve.

Detection of the leakage/break is by an alarm on the measured level in the safeguard building sump .

3.1.10.7. LOCA leading to a containment bypass on the REN [NSS] / RPE [NVDS] / RDP [PRT] systems

The breaks outside the containment analysed on these systems may be compensated by the makeup flow of the CVCS.

3.1.10.8. Summary of results

The overall frequency of the LOCA scenarios leading to a containment bypass is evaluated as $3.72\ 10^{-9}$ /(r.yr) in at power states and at $3.65\ 10^{-10}$/ (r.yr) in the shutdown states.

Identification of the potential bypass initiating events studied in this section is supported by functional analysis and quantification of the initiating events.

As the overall corresponding risk is evaluated at 10^{-9}/r.yr, these scenarios can be considered as'practically eliminated'.

3.2. SUMMARY

The following table provides the distribution of core damage frequencies between the various groups of initiating events:

Groups	Sub-groups	Core damage Frequency (/r.yr) States A,B	Core damage Frequency (/r.yr) States C,D,E	Core damage Frequency (/r.yr) groups	Contrib. (%)
LOCA	Loss of primary cooling Accident	$1.37\ 10^{-07}$	$4.44\ 10^{-10}$	**$1.37\ 10^{-07}$**	23
BYPASS	LOCA leading to containment bypasses	$3.72\ 10^{-09}$	$3.65\ 10^{-10}$	**$4.09\ 10^{-09}$**	-
SSB	Secondary breaks: - Breaks on secondary side (steam or water), - steam line rupture with steam generator tube(s) rupture	$1.89\ 10^{-08}$ $6.21\ 10^{-09}$	- -	**$2.51\ 10^{-08}$**	4
SGTR	Steam generator tube (s) rupture	$1.41\ 10^{-09}$	-	**$1.41\ 10^{-09}$**	-
Secondary system transients	Secondary transients: - total loss of steam generator water supply	$1.10\ 10^{-07}$	-	**$1.10\ 10^{-07}$**	18
LOOP	Total loss of offsite power (2h), Total loss of offsite power (24h), CCF LH	$1.68\ 10^{-09}$ $5.95\ 10^{-08}$ $5.12\ 10^{-09}$	$1.99\ 10^{-11}$ $1.52\ 10^{-08}$	**$8.15\ 10^{-08}$**	14
Primary system transients	Primary transients: - Homogeneous dilution - total loss of SIS cooling in RHR mode, - uncontrolled drop of primary level, - total loss of CVCS pumps.	$2.83\ 10^{-09}$ - - $9.81\ 10^{-09}$	$7.67\ 10^{-09}$ $1.92\ 10^{-10}$ $5.01\ 10^{-09}$ -	**$2.55\ 10^{-08}$**	4
LOCC LUHS	Partial or total loss of cooling systems, Loss of ultimate heat sink.	$3.86\ 10^{-08}$ $4.31\ 10^{-08}$	$1.50\ 10^{-08}$ $2.53\ 10^{-09}$	**$9.92\ 10^{-08}$**	16
ATWS	Anticipated Transients without Scram	$1.24\ 10^{-07}$	-	**$1.24\ 10^{-07}$**	20
Heterogeneous dilution		$5.20\ 10^{-09}$		**$5.20\ 10^{-09}$**	1
TOTAL				**$6.1\ 10^{-07}$**	

Distribution of core damage frequencies in initiating event group

3.3. DISTRIBUTION OF CORE DAMAGE FREQUENCY BY REACTOR OPERATIONAL MODES

The following table shows the distribution of the total CDF according to the various reactor operational modes. It highlights the fact that the full and low power operational modes represent the biggest contribution to the risk.

Reactor states	Description	Core damage frequency (/r.yr.)	Contribution	States power on/shutdown
A - B	AT-POWER STATE UP TO INTERMEDIATE SHUTDOWN ABOVE 120°C	**$5.62\ 10^{-7}$**	92.5%	92.5%
C	INTERMEDIATE SHUTDOWN AND COLD SHUTDOWN WITH RHR OPERATING	**$1.32\ 10^{-8}$**	2%	7.5%
D	COLD SHUTDOWN WITH RCS OPEN	**$3.10\ 10^{-8}$**	5.5%	
E	COLD SHUTDOWN FOR REFUELLING	**$3.18\ 10^{-10}$**	-	
TOTAL		**$6.1\ 10^{-7}$**		

Distribution of CDF by reactor operational modes

3.4. CONCLUSIONS

The overall EPR core damage frequency is evaluated at $6.1\ 10^{-7}$/r.yr for internal events

This result is in accordance with the probabilistic objectives stated in Sub-chapter R.0.

Preventive maintenance contributes approximately 15% of the overall core damage frequency. This is consistent with the requirement expressed in the Technical Guidelines (see Section C.1.2) that ‘outages due to preventive maintenance should not contribute a significant proportion of the overall core damage frequency’.