UK EPR	Title: PCSR – Sub-chapter 15.1 – Level 1 PSA		
	UKEPR-0002-151 Issue 05		
Total number of pages: 225		Page No.: I / V	
Chapter Pilot: F.GODEFROY *Name/Initials*	*Date* 08-11-2012		
Approved for EDF by: A. MARECHAL *Name/Initials*	*Date* 09-11-2012	Approved for AREVA by: G. CRAIG *Name/Initials* G Craig	*Date* 09-11-2012

REVISION HISTORY

Issue	Description	Date
00	First issue for INSA review	08-01-08
01	Integration of co-applicant and INSA review comments	30-04-08
02	PCSR June 2009 update: - Clarification of text - Inclusion of references - Change in description of plant operating states (section 3.1 and Section 15.1.3 - Table 1) - Change in reliability data used in the PSA (section 3.2 and Section 15.1.3 - Table 2) - Integration of preventative maintenance in the base line PSA model (section 3.6 and all sections with results) - Update the initiating events list: o 2A-LOCA in the base line PSA model (sections 4.1.1. and 4.2.1) o Medium LOCA frequency updated (section 4.2.1)	27-06-09
03	Removal of RESTRICTED marking and addition of CCI marking.	18-06-10
04	Consolidated Step 4 PCSR update: - Minor editorial changes - Clarification of text - Update and addition of references - Update of description of I&C modelling consistent with PSA update: updated I&C reliability data and addition of the NCSS platform (§3.4 and Section 15.1.3 – Table 3) - Update of reliability data used in the PSA, including reliability of the MHSI pumps (§3.2 and Section 15.1.3 - Table 2) Continued on next page	31-03-11

REVISION HISTORY (Cont'd)

Issue	Description	Date
04 cont'd	Consolidated Step 4 PCSR update (cont'd): - Update of initiating event descriptions and frequencies (Section 15.1.4 – Table 4). - Update of Level 1 PSA (§5 and §6)	
05	Consolidated PCSR update: - References listed under each numbered section or sub-section heading numbered [Ref-1], [Ref-2], [Ref-3], etc - Minor editorial changes - Update of text and cross-references consistent with PCSR changes with respect to heterogeneous dilution safety case (§4.6.2.1, §5.8.4.2.2)	09-11-2012

Text within this document that is enclosed within curly brackets "{…}" is AREVA or EDF Commercially Confidential Information and has been removed.

This document has been prepared by or on behalf of AREVA NP and EDF SA in connection with their request for generic design assessment of the EPR^{TM} design by the UK nuclear regulatory authorities. This document is the property of AREVA NP and EDF SA.

Although due care has been taken in compiling the content of this document, neither AREVA NP, EDF SA nor any of their respective affiliates accept any reliability in respect to any errors, omissions or inaccuracies contained or referred to in it.

Trade Mark

EPR^{TM} is an AREVA Trade Mark.

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 15.1 – LEVEL 1 PSA

1. INTRODUCTION

This sub-chapter covers the scope and definition of internal initiating events considered in the Level 1 PSA, and presents the methodology and results. Results are presented in terms of Core Damage Frequency (CDF) per reactor per year.

The probabilistic safety objectives adopted for the UK EPR are stated in Sub-chapter 15.0.

Probabilistic studies were carried out during the EPR design process to support and optimise the design of systems and processes. This has allowed a well-balanced system and process design to be achieved. It has also provided a reasonable assurance that the plant complies with the stated safety objectives.

In the PSA, fault trees are used to estimate the failure probability of the system missions. Event trees are used for estimating the Core Damage Frequency (CDF) due to each initiating event.

The risk quantification is carried out using RiskSpectrum® Professional software [Ref-1], version 2.10.04. This software suite has been developed by the Swedish company RELCON. It enables the modelling of fault trees to be integrated with the event tree modelling. The code models sequence dependencies automatically.

2. SCOPE

The Level 1 PSA analysis addresses all potential accidents related to the reactor core that could lead to radioactive releases in the plant. Results, in terms of Core Damage Frequency per reactor year [/ry], are presented in sections 5 and 6 of this sub-chapter.

The scope of the probabilistic study presented in this sub-chapter is defined below:

- All reactor operational modes are covered, from operation at full power to shutdowns for refuelling with at least one fuel element in the reactor vessel;

- The study in this sub-chapter is limited to internal events. The internal initiating events considered are presented and justified in section 4 of this sub-chapter. Internal and external hazards are addressed in Sub-chapter 15.2;

- Thermal-hydraulic and neutronic parameters, initial conditions, set-points and component availabilities are based on best-estimate data.

The probabilistic analysis of fuel damage in the spent fuel storage pool is presented in Sub-chapter 15.3.

The methodology used to model the plant is presented in section 3 of this sub-chapter. The model considers:

- Random individual component failures;
- Components which fail as a result of the initiating fault;
- Common cause failures (involving both components and signals);
- Pre-fault human errors and human errors occurring during the course of fault sequences. The Human Reliability Analysis methodology is presented in section 3.5 of this sub-chapter;
- Potential dependencies between separate human activities;
- Other dependencies. (The analysis of the support systems is presented in section 3.6 of this sub-chapter).

Equipment unavailabilities due to repair and preventive maintenance activities during at-power and shutdown states are included in the base case PSA model. The impact of the preventive maintenance programme on the PSA results is discussed in Sub-chapter 15.7.

Uncertainty analyses using a Monte-Carlo methodology are performed to derive confidence levels for the PSA results. The analyses take into account uncertainties in reliability data and initiating event frequencies by inputting these parameters as probability distributions. The overall conclusions of the PSA analysis, including uncertainties, are presented in Sub-chapter 15.7.

The sensitivity of the PSA results to major assumptions and expert judgments are also presented in Sub-chapter 15.7.

3. METHODOLOGY

3.1. PLANT OPERATING STATES

3.1.1. Introduction

The plant passes through multiple configurations during a cycle and a series of “standard reactor states” have been defined corresponding to these different configurations. In order to make the number of reactor states to be analysed manageable, the states are grouped using a qualitative assessment. The general approach to grouping is that within a standard reactor state there should be:

- Similarity of plant parameters;
- Similarity of available systems and components;
- Similarity of potential initiating events.

In some cases, plant conditions such as pressure, temperature, system availabilities, decay heat level etc. may change with time within one reactor state. In such cases, conservative assumptions are generally made in the analysis.

3.1.2. Scope

All standard reactor states are addressed in the PSA from full power operation to cold shutdown operation. Data is obtained from the EPR Basic Design Report [Ref-1] and more recent AREVA information related to the EPR design and operating procedures. The standard reactor states are given in Section 15.1.3 - Table 1. This table provides the status of the main systems and components, including the containment, and the durations of the shutdown states considered in the PSA.

The durations of the different states are averages per year, assuming an 18 month fuel cycle and an 18 day refuelling outage. Allowance is made for additional plant unavailabilities for inspections (e.g. turbine inspections, 10 year inspections) repairs and tests which lead to outage durations longer than those of a standard refuelling outage.

3.1.3. Overview of the Standard Reactor States

3.1.3.1. Power State (A, B)

In most cases, the present PSA studies for power states address reactor states A and B together, because similar functional analyses apply. The exceptions are the following (see section 4 of this sub-chapter):

- Boron dilution events which are studied separately for states A and B;

- Loss of main feedwater, loss of condenser, turbine trip, anticipated transient without scram and the reactor trip, which are studied only for state A;

- Loss of the Start-up and Shutdown System which are studied only in state B.

In states A and B, the plant is assumed to be at full power (i.e. 4500 MWth), with all systems available, all controls in operation, and the core thermal power being removed via the steam generators.

The average time spent in standard reactor states A and B represents 94% of the cycle duration.

Preventive maintenance is technically possible during power operation and is permitted on some safety systems (see section 3.6.1 of this sub-chapter).

3.1.3.2. Shutdown States (C, D, E, F)

For these states the plant condition considered in the PSA model represents plant shutdown rather than plant start-up. For example during plant start-up in State Ca, four reactor coolant pumps are in operation to heat up the reactor coolant and only two RHR trains are in operation. The PSA models the corresponding shutdown configuration (two reactor coolant pumps and four RHR trains in operation) since the core thermal power is much greater during plant shutdown than during plant start-up.

3.1.3.2.1. Shutdown State Ca

State Ca is representative of cold shutdown with the residual heat removal system in operation for reactor cooling. The reactor is pressurised and full of water.

PSA state Ca represents the different plant configurations presented in Section 15.1.3 - Table 1. The following configuration is modelled in the PSA:

- 4/4 residual heat removal trains in operation;
- 2/4 steam generators available;
- 2/4 reactor coolant pumps in operation;
- Reactor coolant temperature = 120°C;
- Reactor coolant pressure = 3.0 MPa;
- Reactor coolant system closed and full;
- Containment hatch opened or closed.

A plant configuration with the pressuriser full of water (so-called water solid condition) is assumed in PSA state Ca. This plant configuration occurs briefly during plant outages (i.e. for about 5 hours during a normal refuelling outage). Overpressure transients in water solid operation are considered in section 3.6.1 of this sub-chapter.

Some preventive maintenance is performed on the steam generators during state Ca and Cb (see section 3.6.1 of this sub-chapter).

3.1.3.2.2. Shutdown State Cb

State Cb is representative of 3/4 loop operation (usually called mid-loop operation), with the reactor pressure vessel head in place. In this state, the water inventory has been manually reduced for operational purposes. The pressure is reduced to 0.1 MPa but the reactor coolant system is capable of being pressurised and the steam generators are available for residual heat removal.

3.1.3.2.3. Shutdown State D

State D represents 3/4-loop operation with the reactor pressure vessel head removed. The water inventory is increased from the 3/4-loop to reactor pool flooded level {CCI} [a] in this plant state: however for the PSA analysis the reactor coolant level is conservatively assumed to be at its lower limit for 3/4 loop operation.

As the vessel head is open, the secondary side systems cannot be used for residual heat removal.

3.1.3.2.4. Shutdown State E

State E is representative of core loading and unloading operations. The reactor pool is full to the {CCI} [a] level. Fuel elements are moved from the vessel to the fuel building during core unloading and from the fuel building to the vessel during core loading.

Some preventive maintenance is performed on safety and operating systems in State E (see section 3.6.1 of this sub-chapter).

3.1.3.2.5. Shutdown State F

State F is representative of the condition with all fuel assemblies outside the reactor building. No accidents involving core damage in the Reactor Building are studied for this state. This state is used only for consideration of fuel pool cooling accidents.

3.2. RELIABILITY DATA

Reliability data [Ref-1] are derived mainly from operational experience feedback from France and Germany, supplemented by data from the EG&G generic reliability database.

Reliability data used for instrumentation and control systems are defined in section 3.4 of this sub-chapter.

Failure modes and related reliability data used for equipment other than instrumentation and control systems are detailed in the UK EPR data report [Ref-1]. For each component type, the component boundary is presented according to the definition given in the relevant source. The UK EPR PSA fault tree modelling in the system analyses is consistent with these component boundaries.

The UK EPR data report [Ref-1] presents the rationale for the database selection. Broadly, the methodology adopted in the UK EPR PSA uses parameters taken from the EDF database. In the absence of EDF data, or if the component is similar to equipment used in German plants and is included in the ZEDB database [Ref-2] [Ref-3], the latter is used. When no relevant EDF or ZEDB data exist, reliability data are taken from the EG&G database [Ref-4]. Ultimately conservative data are assumed.

The reliability data used in the UK EPR Level 1 PSA are summarised in Section 15.1.3 – Table 2.

3.3. COMMON CAUSE FAILURES

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

CCF applies to groups of redundant equipment items operating under similar conditions.

The same CCF model is used for different types of component: pumps, valves, diesels, high and medium voltage circuit breakers, sensors etc.

No account is taken of a CCF of equipment items in the following cases:

- when items of equipment are not required to change state during an accident (e.g. switchboards, piping etc). For example simultaneous leakage due to corrosion of pipework in four redundant trains, is not considered as a CCF. It is considered that such leakages could occur at any time, and hence it is likely that the damage would be detected during normal operation, leading to a programme of repair and prevention on the redundant equipment in the trains.

- when several components, such as contactors and emergency switchgear, are operating under similar conditions before the initiator occurrence. In this case the failures modes would be likely to be detected by observation, allowing corrective measures to be carried out.

CCF of components is considered when the components belong to the same system and have the same function. For example CCF of the low-voltage circuit breakers of the MHSI pumps is considered in the modelling of the MHSI system. CCF of the same component belonging to different systems is not considered because such components would have different functions and be subject to different test and maintenance regimes. Therefore, for example, CCF of the low-voltage circuit breakers of the MHSI pumps and similar equipment on other systems (e.g. the ASG [EFWS] pumps) is not considered.

CCF parameters are taken from the European Utility Requirements [Ref-1].

3.4. INSTRUMENTATION & CONTROL

The important role played by the instrumentation and control system is modelled in the PSA by using a specific I&C reliability model called the ‘Compact Failure Model’.

PSA modelling of the I&C systems is implemented in two stages:

- modelling of the I&C control channels with the ‘Compact Failure Model’,

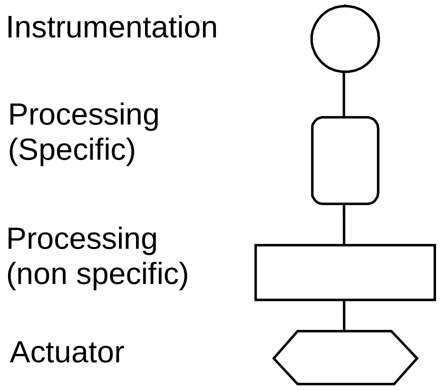
- global integration of the I&C functions into the PSA model.

These two stages are described below.

3.4.1. Methodology

The method of modelling instrumentation and control is referred to as the ‘Compact Failure Model’ (CM), which is a simplified functional representation of the I&C digital systems in the Probabilistic Safety Assessment (PSA).

The CM is based on splitting the I&C digital system into elementary I&C functions, also called channels, each one being represented by a specific fault tree in the PSA. According to the CM, each single I&C function is broken down into three main parts, as shown in the following symbolic representation: an instrumentation part, a specific and non-specific processing part, and an actuator part.



Symbolic representation of an automatic I&C function

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 are used for the overall unavailabilities of the instrumentation and processing parts. These values depend on the classification and are directly used in the PSA Boolean modelling.

3.4.1.1. Instrumentation part

The instrumentation part corresponds to the sensors used as input to the I&C functions. The term “sensors” includes the measuring cell module, the electronic converter and the transmission connector technology.

Modelling of the instrumentation part does not exactly conform to the CM principle. The CM principle recommends modelling the instrumentation part by using groups of redundant sensors. However, in the GDA Step 4 PSA, for a given I&C function, all the sensors required for the elaboration of the signal are separately modelled. When redundant sensors exist, a logic gate is used in order to represent the voting logic between the sensors. Various types of redundancy and voting logic are modelled in the UK EPR PSA (for example 2 out of 4, 2 out of 3 or 1 out of 2).

Some exceptions exist where a single basic event is used to represent several sensors (for example, rod position sensors or Self Powered Neutron Detectors). More details about these exceptions can be found in UK EPR I&C report [Ref-1].

3.4.1.2. Processing part

The processing part corresponds to the processing functions implemented in the following computerised I&C systems: the Protection System (RPR [PS]), the Safety Automation System (SAS), the Process Automation System (PAS), the Reactor Control Surveillance and Limitation System (RCSL) and the Severe Accident I&C (SA I&C). These functions receive a signal from the instrumentation part.

According to the CM rules, the processing part of a given I&C system is divided into two parts: the specific processing part and the non-specific (also called “common”) processing part.

The specific processing part relates to a given safety function and its processing logic. It 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) used by the associated safety function and required for partial instructions.

The non-specific processing part takes into account all the components used for voting processing. It includes, moreover, all the elements, systems and common protocols necessary for data transmission (e.g. the data buses, the exchange protocols). This part also includes the representation of common equipment points as well as Common Cause Failures that may be introduced by use of common technology.

The Reactor Protection System (RPR [PS]) is divided into two sub-systems, A and B: all the signals processed in a given sub-system are affected by the failure of this sub-system. It is assumed in the PSA that the specific logic parts of the RPR [PS] are represented by the two RPR [PS] diverse sub-systems: RPR [PS] sub-system A and RPR [PS] sub-system B. Therefore the specific logic part of a given RPR [PS] channel corresponds to the RPR [PS] sub-system in which the signal is processed. Furthermore the failure of the common part of an RPR [PS] channel corresponds to failure of the whole TXS platform.

Since the RCSL and SA I&C are part of the TXS platform, their common part failure is the same as for the RPR [PS]. Additionally, specific processing failures are modelled for each type of RCSL or SA I&C signal.

3.4.1.3. Actuator part

The actuator part corresponds to the elements that support the action on the process sub-function. It represents set of actuators (pumps + motor, valves + drive) and includes their associated electrical interface (switchgear) and the I&C part supporting the basic actuator control sub-functions.

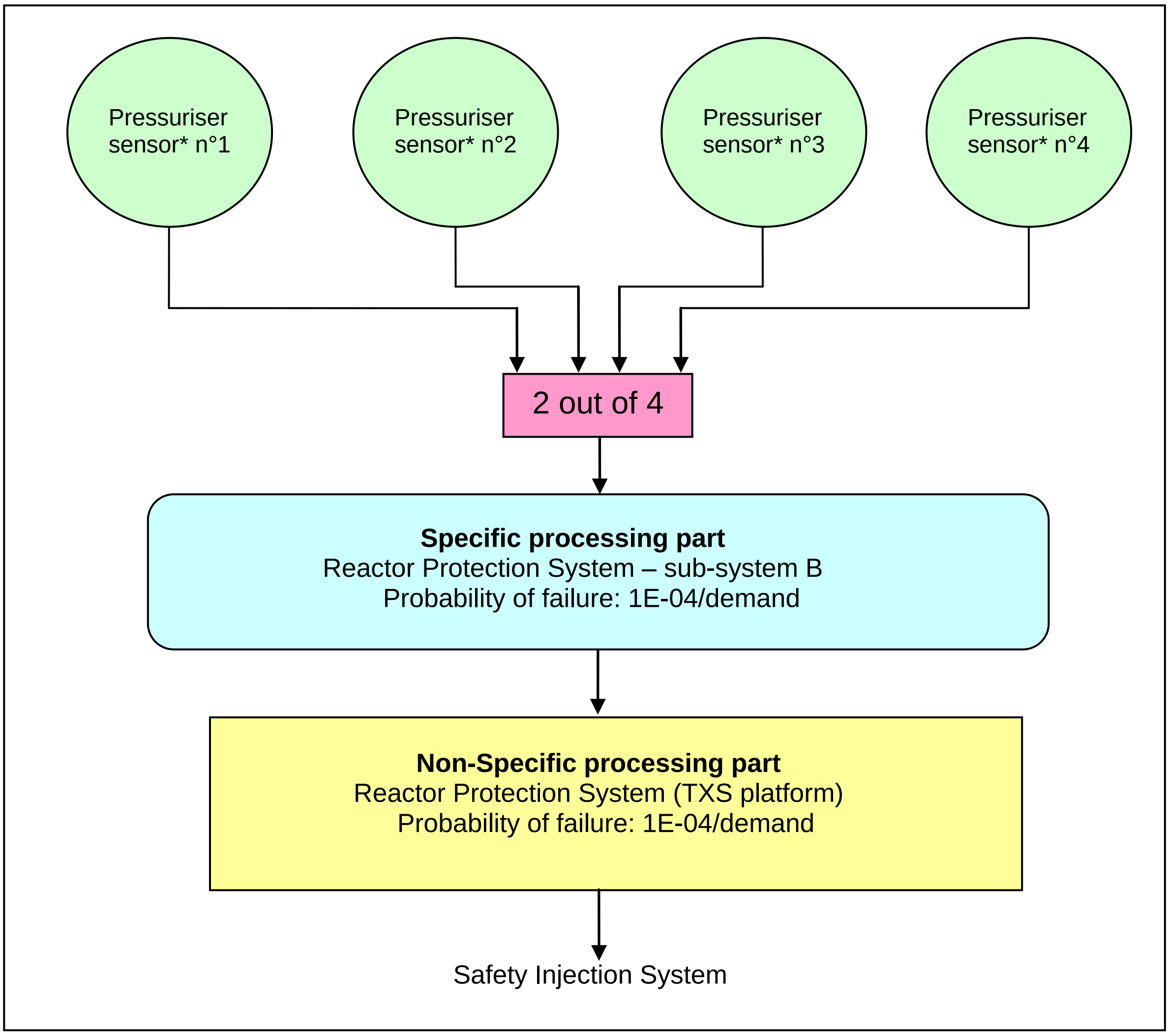
The actuators themselves are not included in the actuator part.

The number of actuator trains depends on the degree of redundancy of the mechanical or electrical system supporting the safety function.

At present, the actuator part is not modelled in the GDA Step 4 PSA model. Since modelling of the actuator part is not dealt with in the CM, this actuator part will be considered during modelling of the related specific systems (and not in the I&C modelling), when the detailed allocation of acquisition controls is specified.

3.4.1.4. Example of implementation of the CM

The following figure gives a symbolic representation of a signal actuated by the protection system (RPR [PS]). This example is based on the detection of a low pressure in the pressuriser by four sensors with a 2 out of 4 voting logic. The signal is processed in sub-system B of the RPR [PS] and actuates the start-up of Safety Injection.


Pressuriser sensor* n°1
Pressuriser sensor* n°2
Pressuriser sensor* n°3
Pressuriser sensor* n°4
2 out of 4
Specific processing part
Reactor Protection System – sub-system B
Probability of failure: 1E-04/demand
Non-Specific processing part
Reactor Protection System (TXS platform)
Probability of failure: 1E-04/demand
Safety Injection System

Symbolic representation of the RPR [PS] safety function: Safety injection actuation on low pressuriser pressure

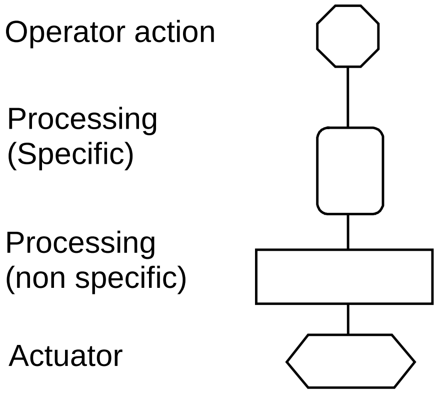
3.4.1.5. Extension of the Compact Model

The basic Compact Model does not represent some specific elements such as the Human-Machine Interface (HMI) and the hardwired Non-Computerised Safety System (NCSS) I&C platform. Therefore, some additional items have been implemented into the GDA Step 4 PSA model in order to model the HMI and the NCSS, whilst remaining consistent with the modelling principles of the CM.

3.4.1.5.1. Modelling of the Human Machine Interface

Every human action modelled in the PSA, with the exception of manual reactor and turbine trip, some specific operator actions performed local to plant, and actions implemented in the NCSS (see sub-section 3.4.1.5.2 below), relies on the computerised I&C systems (TXS and/or SPPA-T2000). Moreover the failure of the SPPA-T2000 platform results in the unavailability of the majority of the manual controls of the plant performed through the Human-Machine Interface; indeed only a few manual actions are available through the TXS platform. For example, manual RBS [EBS] start-up, manual ASG [EFWS] start-up and manual containment isolation are available through the TXS platform, whilst manual start-up of safety injection is not. Since the total loss of computerised I&C would remove the capability for operator recovery from the Main Control Room (MCR) or Remote Shutdown Station (RSS), this situation is modelled accordingly in the PSA. Thus performance of a given human action depends on the non-failure of its relevant associated I&C systems.

A modelling structure similar to the one used for automatic function modelling has been chosen to represent operator actuated functions. Therefore, the complete channel of an operator action performed in the MCR or RSS can be represented as follows:



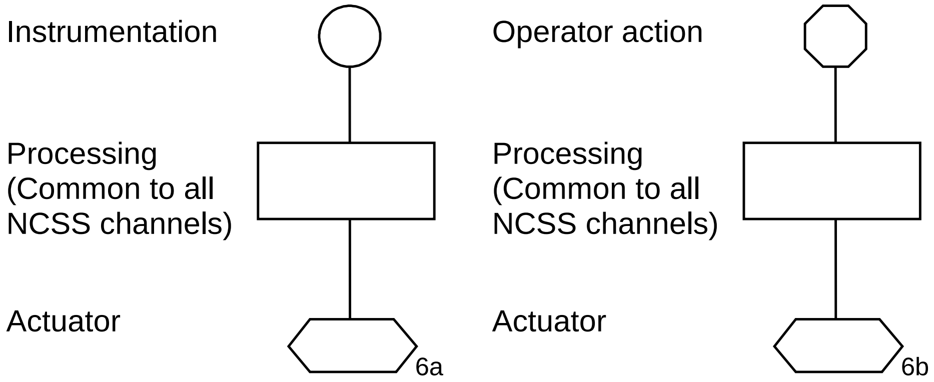
Symbolic representation of a manual I&C function

Detailed modelling of operator actions and their related I&C channels is described in the UK EPR I&C report [Ref-1].

3.4.1.5.2. Modelling of Non Computerised Safety System

The NCSS is a third I&C platform (in addition to the TXS and SPPA-T2000 platforms), whose distinctive feature is hardwired technology. It is claimed as a backup in case of total loss of the computerised I&C. Both automatic safety functions and operator actions are implemented in the NCSS.

It is considered that the failure of the specific processing part of the NCSS is covered by the failure of the whole NCSS technology. Therefore, a NCSS channel is modelled in the GDA Step 4 PSA using the following structure:


Instrumentation
Operator action
Processing (Common to all NCSS channels)
Processing (Common to all NCSS channels)
Actuator
Actuator
6a
6b

Symbolic representation of a NCSS I&C function (6a: automatic function/ 6b: manual function)

The NCSS instrumentation is modelled in the same way as for safety functions processed by computerised I&C. As the NCSS functional requirements do not yet specify the sensors that will be used as inputs to the automatic I&C signals, it is assumed that RRC-A sensors are used whenever possible. If not, RPR [PS] sensors are used instead. Justification for this choice is given in UK EPR I&C report [Ref-1].

The major assumptions made for the modelling of operator actions performed through the NCSS dedicated panel are presented in sub-section 3.4.3.2 below.

The processing part of the NCSS is considered as a single unique part (no distinction is made between specific or non-specific logic parts) common to all NCSS channels: automatic functions and manual actions. A failure of this processing part leads to total loss of all NCSS actions.

3.4.2. 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 in accordance with the equipment classification. An unavailability value is specifically assigned to each I&C system. These values are based on I&C reliability studies performed in the preliminary design phase of the system, updated during the detailed design phase in order to take into account the final architecture.

EDF/AREVA consider the reliability values in this study are conservative and may not be fully representative of the actual performance of the digital I&C used within the UK EPR I&C system. However, the values recognise the necessity to limit the claims on computer-based systems because of the need to provide an adequate safety justification of their performance. Therefore, the actual risk levels may be lower than those substantiated in the justification.

3.4.2.1. Instrumentation part

The justification of reliability claims for sensors is given in the UK EPR I&C report [Ref-1]. The numerical values of the instrumentation part take account of the following:

- The hourly failure rate of sensors according to the EG&G database and as validated by EDF experience,
- Calibration errors,
- The efficiency of the internal self-tests conducted within the logic part,
- The Operating Technical Specifications, and the time interval between the periodic tests,
- The general quality of the system (reconfiguration etc...).

The following table presents the values implemented in the GDA Step 4 PSA model:

Unavailability values for instrumentation part

{CCI removed}

If a function requires N groups of sensors, the risk of unavailability of the instrumentation part will be multiplied by N. Furthermore, Common Cause Failures between redundant sensors are included in the PSA model.

3.4.2.2. Specific processing part

The reliability claims on the specific logic parts takes account of the following:

- System internal architecture and logic (degree of redundancy, etc…),
- The possibility of design errors,
- Independent failure rates and Common Cause Failures of equipment affecting redundant components (e.g. 4 boards for four-fold redundancy),
- Failures due to software packages specially developed for a given system and for a specific requirement. These packages include application software which requires the development of a specific logic (e.g. threshold overshoot, taking account of particular operating conditions, use of permissives),
- Internal diagnosis self-test frequency,
- Human errors in data input.

Taking the above factors into account the following values are implemented in the GDA Step 4 PSA model:

Unavailability values for specific processing part

{CCI removed}

a

The failure rate of the specific processing part of the SPPA-T2000 is neglected in the PSA model as this failure mode is insignificant due to the highly conservative figures assigned to the failure probability of the whole SPPA-T2000 platform (see section 3.4.2 above).

3.4.2.3. Non-specific processing part

Assigning reliability claims on the non-specific processing parts depends mainly on the class of the considered I&C controllers. The values assigned allow for:

- Common Cause Failures due to errors in the operating software and data exchanges on the network,
- Failures in internal common elements 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…)

Three different common processing parts are considered in the GDA Step 4 PSA model, each corresponding to a type of I&C technology: TXS, SPPA-T2000 or hardwired technology. The following values are implemented in the GDA Step 4 PSA model:

Unavailability values for non-specific processing part

{CCI removed}

a

No additional penalty due to Common Cause Failure between the TXS and SPPA-T2000 digital platforms is considered, as independent failures of both platforms is already considered to have a high probability of occurrence ({CCI removed} [a]).

3.4.3. Integration of the Instrumentation and Control systems in the PSA model

3.4.3.1. Scope

This section details how the CM principles and reliability data have been implemented in the Risk Spectrum model in order to model the UK EPR I&C.

The I&C channels modelled in the GDA Step 4 PSA are of three different types:

- Automatic signals generated by sensors and corresponding orders sent to actuators,
- Monitoring signals generated by sensors and displayed in the MCR,
- Signals generated by operator actions in the MCR and corresponding orders sent to actuators.

The automatic and monitoring signals modelled in the GDA Step 4 PSA are listed in Section 15.1.3 – Table 3.

Permissive and conditional signals

The unavailability of permissive signals is not taken into account as their effect is considered to be negligible. A permissive signal is generally representative of a stable plant state and its unavailability would consequently be detected during normal operation. Therefore, the risk due to an independent failure of a permissive signal coinciding with a failure of protection signals during a transient is assumed to be insignificant.

3.4.3.2. PSA modelling assumptions

Structure and inclusion of I&C modelling in the PSA

Each I&C channel (automatic signal or operator action through HMI) is modelled in one specific fault tree. This fault tree can either be associated with a Function Event and thus be incorporated in an Event Tree, or be directly introduced into a system fault tree.

In a configuration where the initiating event is considered in states ‘A and B’, the I&C signals considered are those applicable in state A.

Human factors analysis

Operator recovery after I&C failures during accidents

In many I&C automatic mission failures, operator action is credited in as a recovery measure in the PSA.

A preliminary analysis of the potential operator prompts (alarms and indications in the Main Control Room) has been carried out in the Human Reliability Analysis report [Ref-1]. At present, manual actions are mostly modelled in the PSA without taking into account any dependency on these prompts:

- It is assumed that diagnosis is performed using prompts which are sufficiently diverse from those used to generate the automatic I&C actions that the manual action replaces,
- Dependency of operator action on the HMI is modelled as described in section 3.4.1.5.1, which covers processing of the monitoring signals,
- The failure probability of the prompt is generally included in the reliability value assigned to the operator action.

Operator recovery after I&C failures during normal operation

Operator recovery is taken into account in the reliability data of the acquisition part using the Mean Time To Repair (MTTR), which is dependent on the location (Reactor Building or Electrical building) of the related instrumentation.

Power supply modelling

The I&C power supply dependency is introduced in the PSA model by modelling a failure of the safety functions when one or more power supply divisions fail. The voting logic modelled between the different power supply divisions represents the voting logic between sensors used as input to the function. More details about power supply modelling in the I&C fault trees can be found in UK EPR I&C report [Ref-2].

As it is much more complex to define which electrical divisions supply the I&C that process signals resulting from manual operator actions, a two out of four logic between the four I&C power supply divisions is modelled for each operator action.

NCSS sensors

RRC-A sensors are modelled as inputs to the NCSS automatic functions whenever possible. If it is not possible to use RRC-A sensors, RPR [PS] sensors are used instead. An analysis that justifies this choice of modelling is presented in UK EPR I&C report [Ref-2].

NCSS operator actions modelling

Assumptions made in modelling NCSS operator actions are listed below:

- For any operator action performed using the NCSS panel, a stress penalty is applied.

- The time window available for any operator action performed through the NCSS is reduced by 10 minutes in comparison with the similar action performed in normal operation. This delay allows for the time needed by the operator to diagnose the loss of computerised I&C.

- No stress penalty is considered for severe accident actions performed from the MCR (OSSA actions).

- Following a loss of the SPPA-T2000 platform, a switchover to the NCSS panel is assumed even if the TXS platform is still available.

3.5. HUMAN RELIABILITY ANALYSIS

The HRA [Ref-1] is largely based on the methodology developed by Swain in the Accident Sequence Evaluation Program (ASEP) Human Reliability Assessment (HRA) Procedure [Ref-2]. It involves considering pre-accident and post-accident tasks.

The following types of human actions are considered in the PSA:

- Pre-accident tasks (errors due to maintenance)

- Post-accident tasks (operator actions)

Human errors causing an initiating event are analysed in section 4 of this sub-chapter.

3.5.1. Pre-Accident Tasks

Pre-accident errors are considered in the system analyses. The probability of such errors is quantified by:

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

where P_b = basic human error probability for pre-accident tasks,

P_{NR} = probability of non-recovery depending on factors favouring recovery.

3.5.1.1. Basic human error probability

P_b is set at 0.03 per demand as a conservative value. This figure represents the combination of a generic human error probability of 0.02 per demand assessed for an error of omission and a probability of 0.01 per demand assessed for an incorrect performance of a task. It also assumes that an error of commission is always possible if no error of omission occurs. Thus, for each critical action that has to be accomplished, P_b is 0.03 per demand. This value covers errors in positioning actuators (valves, circuit breaker racked-out ...).

Failure to perform a critical step in a calibration procedure (calibration of I&C or of an actuator, pressure setting of a relief valve ...) is not assessed as a pre-accident human error in the PSA. The calibration errors are considered in the derivation of the failure rate of the instrumentation part (see sub-section 0 of this sub-chapter).

3.5.1.2. Probability of non-recovery

To assess the effects of recovery actions on P_b, four categories of recovery factors are defined (alarm, checks, administrative controls or periodic tests etc). A probability of non-recovery P_{NR} is associated with each category as shown in the following table.

Probability of non-recovery (P_{NR}) for pre-accidental tasks

CATEGORY	ELEMENT EXAMPLES FAVOURING RECOVERY	{CCI}[a]
1	Category 1 alarm (visual and sound warning) Key lock with supervision of the key Anomaly detectable by checks planned during standard state changes	{CCI}[a]
2	Periodic test Large change in the value of parameter recorded during each shift Commissioning and requalification enabling the anomaly in question to be effectively detected	{CCI}[a]
3	Indication of position in control room Alarm of category other than 1 (on screen)	{CCI}[a]
4	None of the above factors	{CCI}[a]

3.5.2. Post-Accident Tasks

Post-accident tasks are those which are performed by the operators to return the plant to a safe condition. This category includes diagnosis tasks and post-diagnosis tasks. The probability (P) of failure of a post-accident task is:

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

where : P_d = probability of a false diagnosis,

P_a = probability of an incorrect action when the diagnosis is correct,

P_{NRa} = probability of non-recovery having performed an incorrect action.

3.5.2.1. Diagnosis Model

The diagnosis phase includes the detection of the accident, the diagnosis itself, decision making and selection of an Emergency Operating Procedure (EOP). T_d is the estimated time to make the diagnosis and take these related actions. This period starts at the first significant alarm or provision of information provided to the operator. The probability of failure of the diagnosis P_d as a function of T_d is provided in Section 15.1.3 - Table 4. P_d is a joint human error probability (HEP) representing the whole operating team in the Main Control Room (MCR). This table was derived from the Swain's curve assuming the median joint HEP curve [Ref-1]. Such a table enables a value of $P_d(T_d)$ to be derived more precisely than by using a curve.

3.5.2.2. Time dependency between diagnosis and post-diagnosis actions

T_a is the estimated time needed to reach the proper location inside or outside the MCR and to perform the required actions following a correct diagnosis. T_a is estimated {CCI removed} [a] for an action performed within the MCR.

Actions performed outside the control room are not modelled, except for:

- Local opening of the Main Steam Relief Trains in the steam valve room together with the cross-connection of the Emergency Feedwater line (5E-02/demand) [Ref-1];
- Start of the Station Blackout Diesel Generators locally in the Diesel Building (5E-02/demand);
- Cross-connection of the Emergency Feedwater Tank locally in the Safeguard Building (1E-04/demand) [Ref-2];
- Local isolation of the leakage in V-LOCA (5E-02/demand);
- Local start-up of an EVU [CHRS] train (5E-02/demand);
- Human Actions considered in the analysis of initiating events leading to loss of fuel pool cooling.

$T_m = T_d + T_a$ is the maximum available time taken to perform the diagnosis and complete the necessary actions. T_m is based either on the thermo-hydraulic analyses, if available, or estimated using engineering judgement [Ref-1].

3.5.2.3. Post-Diagnosis Tasks

The model involves only the actions taken after the diagnosis has been made. Post-diagnosis actions are those which logically follow a correct diagnosis of the abnormal event. The probability of failure of a post-diagnosis task (P_a x P_{NRa}) depends on the probability of failure of the action (P_a) and of the probability of non-recovery (P_{NRa}) in the case of an incorrect action.

- P_a = 0.05 for critical actions to be performed under “moderately high stress”.

  An operator action is considered as a "moderately high stress" action when it is requested by the EOPs without ambiguity and when the operators are properly trained on simulators for this action. This is the case for the majority of the actions taken into account in the present PSA.

- P_a = 0.25 for critical actions to be performed under “extremely high stress”.

  Primary Bleed-and-Feed actuation is classified as "extremely high stress". In this case the operator might have some hesitation in opening the RCP [RCS]. Such hesitation should not occur when Bleed-and-Feed is required in the event of a LOCA because the RCP [RCS] is already open. However, in this case the same value is conservatively used for P_a.

- P_{NRa} depends on the maximum time available (T_m) to perform the diagnosis and the required action. It also depends on whether a change in important physical parameters explicitly monitored according to the Emergency Operating Procedures (EOP) occurs. In addition, it depends on whether the recovery action is performed from the main control room or outside the main control room. The probabilities used in the PSA are provided in the table below.

Probability of non-recovery (P_{NRa}) in the event of an incorrect action.

	P_{Nra}		
Maximum available time T_m	**{CCI}**[a]	**{CCI}**[a]	**{CCI}**[a]
No major factor is explicitly monitored according to the EOP	**{CCI}**[a]	**{CCI}**[a]	**{CCI}**[a]
Change in important physical parameter explicitly monitored according to the EOP (e.g. SG level, pressuriser level, primary pressure, saturation margin, criticality, ...), recovery action performed within the main control room	**{CCI}**[a]	**{CCI}**[a]	**{CCI}**[a]
Change in important physical parameter, but recovery action performed outside of the main control room	**{CCI}**[a]	**{CCI}**[a]	**{CCI}**[a]

3.5.2.4. Screening of post-accident human actions

Only a few post-accident human actions are modelled in the PSA. They have been determined and selected using the following approach:

1. Recovery actions described in the accident analyses of the Basic Design Report [Ref-1] are modelled in the PSA. These actions have been identified prior to the writing of the emergency operating procedures specific to the EPR design. To determine those actions, typical PWR actions and operating procedures adapted to the EPR design have been used.

2. Recovery actions with a time window shorter than 30 minutes are not considered in the deterministic safety analysis but are modelled in the PSA if:

   a. they are a backup to an existing automatic action and
   b. there are sufficiently clear indications available to the operator and
   c. the time window is greater than 10 minutes.

3. Additional recovery actions have been identified using expert judgment of PSA and EOP experts.

Only the recovery actions are addressed for the GDA process, the actions of commission due to misdiagnosis are not modelled.

3.5.2.5. Dependency Model

The Swain approach is used to assess the dependencies between human actions.

For post-accident errors, $P_{(B/A)}$ is the conditional probability of an operator error in performing an action B, knowing that the action A has failed. The different levels of dependence are the following:

- "zero" dependence: the probability of failure of the action B does not depend on the success or failure of the action A: $P_{(B/A)} = P_{(B)}$,

- "low" dependence: there is a dependence between the actions A and B, but a complete dependence cannot reasonably be assumed: $P_{(B/A)} = [1 + 19 P_{(B)}] / 20$

- “medium” dependence: $P_{(B/A)} = [1 + 6 P_{(B)}] / 7$

- "high" dependence: there is a strong dependence between the actions A and B: $P_{(B/A)} = P_{(B/A)} = [1 + P_{(B)}] / 2$

- "complete" dependence: $P_{(B/A)} = 1$

In the present model, zero dependence has only been used in the following cases:

- restart of the normal feedwater and feed and bleed actuation in case of loss of the start-up and shutdown system in state B. The start of normal feedwater for SG feed is a current operating practice;

- failure to trip the reactor coolant pumps and other actions in the case of a loss of cooling chain (during power operation);

- Steam Generator isolation and initiation of secondary cooldown to terminate the leakage following a Steam Generator Tube Rupture.

Pre-accident errors involving identical components, e.g. failure due to errors in tests or maintenance, are covered by the CCF model.

3.5.3. Validity of the HRA Model

The human reliability analysis model used in the level 1 PSA (ASEP method) was chosen for the design phase of EPR. This is used to perform an initial assessment of the important Emergency Operating Procedures (EOPs) to be considered. This simple and proven method allows the quantification of the human errors without requiring access to the full set of emergency operating procedures.

The importance of human actions is considered in Sub-chapter 15.7 where sensitivity analyses show that the reliability assumed for important operator actions has only a low impact on the CDF.

An analysis performed using the SPAR-H human reliability analysis method for the Level 2 PSA (see Sub-chapter 15.4) shows that the results given by the ASEP and SPAR-H methods are comparable, giving results of the same order of magnitude.

3.6. SYSTEM MODELLING

3.6.1. Preventive Maintenance

Unavailability due to preventive maintenance has been included in the Level 1 PSA model base case. Additionally, the increase of risk caused by maintenance activities is considered via a sensitivity analysis. The results of this sensitivity analysis demonstrate the robustness of the EPR design and show that the design meets the probabilistic safety objectives.

The sensitivity analysis is described in Sub-chapter 15.7. This sensitivity analysis evaluates the maximum impact on risk of unavailabilities due to preventive maintenance.

The maintenance scenario considers the following preventive maintenance on certain groups of systems. These groups were determined by a functional analysis.

Maintenance during power operation (at power maintenance)

Group A: simultaneous maintenance lasting 28 days in state A is assumed on one train of the following systems:

- Essential Service Water System (SEC [ESWS]);
- Component Cooling Water System (RRI [CCWS]);
- Safety Injection / Residual Heat Removal System (RIS/RRA [SIS/RHR]);
- Fuel Pool Cooling System (PTR [FPCS]).

Group B: simultaneous maintenance lasting 14 days in state A is assumed on the following systems:

- Chemical and Volume Control System (RCV [CVCS]);
- Reactor Boron and Water Makeup System (REA [RBWMS]).

The maintenance of the RCV [CVCS] is not considered in the baseline model. The RCV [CVCS] is an operating system during power operation and is therefore unlikely to be maintained during the at-power state. The impact of maintenance on this group is only considered in the sensitivity analysis.

Group C: maintenance lasting 28 days in state A is assumed on the following system:

- Emergency Feedwater System (ASG [EFWS]).

The dedicated ASG [EFWS] redundant pumps allowing the ASG [EFWS] tank refilling in tanking suction in the fire protection tank (JAC tank) are not subject to preventive maintenance.

Group D: maintenance lasting 7 days during state A is assumed on the following system:

- Start-up and Shutdown System (AAD [SSS]).

The maintenance of the AAD [SSS] is not considered in the baseline model. Maintenance of this system is not planned during power operation.

Group E: a simultaneous maintenance lasting 14 days in state A is assumed on the following systems:

- Dedicated Cooling Chain (SRU [UCWS]);
- Containment Heat Removal System (EVU [CHRS]);
- Fuel Pool Cooling System (PTR [FPCS]) - 3rd train.

Group F: maintenance lasting 28 days in state A is assumed on the following system:

- Emergency Diesel Generator (LHP/Q/R/S [EDG]).

Group G: maintenance lasting 14 days in state A is assumed on the following system:

- Station Blackout Diesel Generator (LJ- [SBO-DG]).

Group H: maintenance lasting 14 days in state A is assumed on the following system:

- Extra-Borating System (RBS [EBS]).

The maintenance of the RBS [EBS] is not considered in the baseline model. The RBS [EBS] is a 2-train safety system and is unlikely to be maintained during the at-power state. The impact of maintenance on this group is only considered in the sensitivity analysis.

Maintenance during plant outages

Group I: Two steam generators are unavailable in state C. The steam generators are cooled and drained to prepare for the work to be undertaken later (inspection). The unavailability assumed in the PSA is very conservative because:

- The SGs are not drained in every outage;
- The SG are available during part of state Ca;

- The corresponding ASG [EFWS] trains could be aligned to the available SGs (This is disregarded in the sensitivity analysis).

Group J**:** simultaneous maintenance on a division during state E:

- Essential Service Water System (SEC [ESWS]);
- Component Cooling Water System (RRI [CCWS]);
- Safety Injection / Residual Heat Removal System (RIS/RRA [SIS/RHR]).

The sensitivity analysis derives the risk profile for the different groups listed above and gives the increase in risk (i.e. increase in CDF) in preventive maintenance.

3.6.2. System Mission Time

The mission time is the elapsed time after the occurrence of the initiating event during which possible failures affecting the PSA mission are considered. The EPR Level 1 PSA models the sequences up to the time when a final state has been reached. The final state considered is based on the acceptance criteria defined in the support studies [Ref-1]. The thermal-hydraulic supporting studies confirm that such a state is reached in a period time much shorter than 24 hours.

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

The EPR PSA model uses a mission time of 24 hours, in line with standard international practice. Mission times of less than 24 hours are only used for components dedicated to power supply (batteries, diesel generators) in the frame of short term LOOP events, which are limited to 2 hours.

Longer mission times are considered in Sub-chapter 15.7 for sensitivity studies.

3.6.3. Support Systems

The support systems facilitate operation of the main systems by providing a power source (electricity, compressed air, etc) and/or by enabling system operation to be maintained (cooling water, ventilation air, etc).

Different support systems are considered and modelled:

- Electrical supplies (high voltage as, for example, LJA);
- Component Cooling Water System (RRI [CCWS]);
- Essential Services Water System (SEC [ESWS]);
- Diversified heat sink for trains 1 and 4 of the LHSI pumps using cooling water circulation from the Safety Chilled Water System (DEL [SCWS]);

- Heat sink of the dedicated intermediate cooling system of EVU [CHRS] (and, in parallel, the third PTR [FPPS/FPCS] train) with cooling water circulation from the Ultimate Cooling Water System (SRU [UCWS]);

- Component Cooling for Conventional Systems (SRI) and Raw Water Cooling system (SEN) (the second cooling the first), to cool the AAD [SSS] pump;

- I&C (see section 3.4 of this sub-chapter).

These support systems are modelled using either one or more fault trees or as a simple basic event. They are linked to the fault trees representing the main systems. For example, RRI [CCWS] and SEC [ESWS] pumps and the electrical power supply to the actuators are linked to the RIS [SIS] system fault trees.

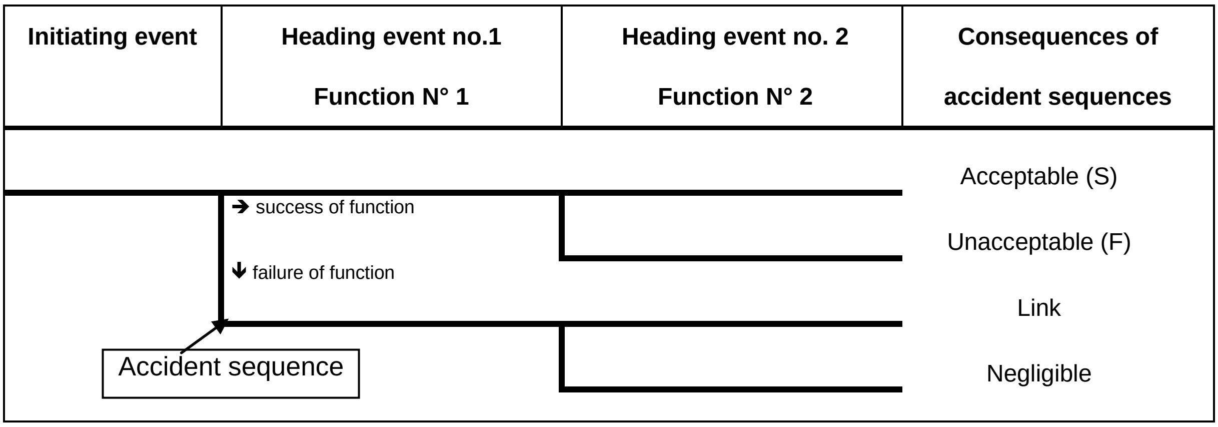
The RRI [CCWS], SEC [ESWS], SRI, SEN and DEL [SCWS] systems and their electrical sources have been the subject of detailed reliability analysis to identify their required missions following different initiating events (e.g. in case of LOOP, loss of ARE [MFWS], small LOCA) [Ref-1].

3.7. ACCIDENT SEQUENCE ANALYSIS

3.7.1. Event Tree Model

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 full event tree comprises all possible accident sequences, i.e. all the accident scenarios following a given initiating event.



Example of the structure of an event tree

Section 15.1.3 – Figures 1 to 3 present some examples of event trees modelled in the PSA.

3.7.2. Consequences

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

For the UK EPR level 1 PSA, the different levels of consequences are defined, as follows

- ‘acceptable consequences’ (S). This indicates that the system functions and human actions carried out in response to the initiating event have ensured that the core damage criteria were not exceeded;

- ‘unacceptable consequences’ (F). These characterise event sequences leading to core damage;

  To satisfy the success criteria in the Level 1 PSA model, each accident sequence must maintain a safe stable state for at least 24 hours. Sequences that do not meet the relevant success criteria are assigned to a core damage end state;

  Core damage is defined as uncovery and heat up of the reactor core to the point at which prolonged oxidation and severe fuel damage involving a large fraction of the core is anticipated;

- ‘link consequences’ or ‘transfers’. This is used when the consequences of an accident sequence are reintroduced into other event tree in the form of an initiating event;

- ‘Not analysed’ (NOT_AN). This end state is applied when the sequence leads to a case that has been already analysed in another event trees. This is only used in the case of induced SGTR for the sequence without SGTR;

- ‘Anticipated Transient Without Scram’ (ATWS). This end state is applied in all at-power event trees. It stops the analysis of event sequences with reactor scram failure as the relevant ATWS scenario are analysed in dedicated ATWS event trees;

- ‘NOT ATWS’. This end state is applied in ATWS event trees where the successive success and failures of RT signals, RT actuators, and mechanical rods leads to the occurrence of the reactor scram. Such events with reactor scram occurrence are not treated as ATWS;

- ‘Undeveloped’ (NOT_DEV). This end state is applied in ATWS event trees where the complete development of sequence analysis would lead to a negligible core damage frequency contribution;

- Very long grace period before core uncovery with steaming in the reactor building (T > 72 hours). This end state is applied in the shutdown states D and E to some event sequences where the successive success or failure of function events leads to core uncovery after a time window of greater than 72 hours.

Decoupling criteria are used to define unacceptable consequences.

All success criteria and decoupling data are defined at the start of each PSA study. Meeting the success and acceptance criteria ensures that the following critical safety functions are met:

- Decay heat removal;

- Reactor coolant system inventory control;

- Reactor coolant system Integrity;

- Reactivity control.

For most transient and LOCA events occurring during power operation, the success criteria for no core damage require the peak cladding temperature in the core to remain below 1204°C. For Anticipated Transient without Scram (ATWS) events, a success criterion of the Reactor Coolant System (RCP [RCS]) overpressure not exceeding 130% of design is also used.

During shutdowns, the success criterion for no core damage is that the core remains covered.

In addition, some further decoupling criteria are considered:

- Long term cooling

  If the residual heat is transferred into the containment e.g. in LOCA events or Feed and Bleed operation, the IRWST temperature must remain below 120°C. This ensures the Safety Injection System (RIS [SIS]) pumps are not damaged.

- Reactivity Control

  In the event of significant rapid overcooling of the primary system RCP [RCS] it is conservatively assumed that the core must remain sub-critical.

The success criteria have been derived from specific supporting analysis [Ref-1].

SECTION 15.1.3 - TABLE 1

Description of Standard Reactor States [Ref-1]

States		Description			Duration
A		From full power to hot shutdown state			8182 h
B		Removal of residual heat by the SGs and cooling of RCP [RCS] to 120°C			43 h
C	Ca	2 LHSI/RHR trains in operation, RCP [RCS] closed and full, containment closed, 4 SGs available, at least 2 reactor coolant pumps in operation $100°C < T_{prim} < 120°C$; $P_{prim} < 3.0$ MPa	26 h	57 h	137 h
		4 LHSI/RHR trains in operation, RCP [RCS] closed and full, containment access hatch open(1), at least 2 SGs available, at least 2 reactor coolant pumps in operation $70°C < T_{prim} < 100°C$; $P_{prim} < 3.0$ MPa	11 h		
		4 LHSI/RHR trains in operation, RCP [RCS] closed, full and water solid, containment access hatch open(2), at least 2 SGs available, 1 reactor coolant pump in operation $\cong 55°C < T_{prim} < 70°C$; $P_{prim} < 3.0$ MPa	13 h		
		4 LHSI/RHR trains in operation, RCP [RCS] closed (repressurisable), containment access hatch closed, at least 2 SGs available, all reactor coolant pumps are stopped $T_{prim} \cong 55°C$; $0.1 < P_{prim} < 0.5$ MPa	7 h		
	Cb	3 LHSI/RHR trains in operation, RCP [RCS] partly open and containment access hatch open(3), at least 2 SGs available, 3/4-loop operation level $T_{prim} \cong 55°C$; $P_{prim} = 0.1$ Mpa	80 h		
D		3 LHSI/RHR trains in operation, RCP [RCS] open, containment access hatch closed (can be open after refuelling), 3/4-loop operation level $T_{prim} \cong 55°C$; $P_{prim} = 0.1$ Mpa			44 h
E		3 LHSI/RHR trains in operation, reactor cavity flooded, containment access hatch open $T_{prim} \cong 55°C$; $P_{prim} = 0.1$ Mpa			121 h
F		Core completely unloaded			233 h

(1) the containment access hatch is open 35% of the sub-state
(2) the containment access hatch is open 40% of the sub-state
(3) the containment access hatch is open 12% of the sub-state

{CCI removed}

{CCI removed}

{CCI removed}

{CCI removed}

{CCI removed}

{CCI removed}

{CCI removed}

{CCI removed}

SECTION 15.1.3 - TABLE 3

Signals modelled in the Level 1 PSA [Ref-1]

Signal description	I&C system	Technology
AUTOMATIC SIGNALS		
High neutron flux rate of change (power range)	PS (Sub-S. A)	TXS
High neutron flux, source range	PS (Sub-S. A)	TXS
Pressuriser pressure < Min2	PS (Sub-S. A)	TXS
Low DNBR (Departure from Nuclear Boiling Ratio)	PS (Sub-S. A)	TXS
High RPE sump level outside containment LHSI train 1	PS (Sub-S. A)	TXS
Loop level < Min1	PS (Sub-S. B)	TXS
Pressuriser pressure > Max2	PS (Sub-S. A)	TXS
∆Psat < Min1	PS (Sub-S. B)	TXS
Pressuriser pressure < Min3	PS (Sub-S. B)	TXS
Containment pressure > Max1	PS (Sub-S. B)	TXS
High core power level > Max3	PS (Sub-S. B)	TXS
High linear power density (HPLD)	PS (Sub-S. A)	TXS
Reactor Coolant Pumps speed < Min1	PS (Sub-S. A)	TXS
SGi level < Min1 NR (i=1 to 4)	PS (Sub-S. B)	TXS
SG1 level > Max2 NR	PS (Sub-S. B)	TXS
SGi level > Max1 NR (i=1 to 4)	PS (Sub-S. B)	TXS
SGi level < Min2 WR (i=1 to 4)	PS (Sub-S. A)	TXS
SGi pressure drop > Max1 (i=1 to 4)	PS (Sub-S. B)	TXS
SGi pressure > Max1 (i=1 to 4)	PS (Sub-S. B)	TXS
SGi pressure < Min1 (i=1 to 4)	PS (Sub-S. B)	TXS
Mechanical blockage of rods	PS (Sub-S. A) PS (Sub-S. B)	TXS
Reactor primary coolant flow rate < Min1	PS (Sub-S. B)	TXS
Cold leg temperature < Min1 WR	SAS	SPPA-T2000
Main steam line 1 activity > Max1	SAS	SPPA-T2000
Antidilution - state A	PS (Sub-S. B)	TXS
Reactor coolant pump i motor upper bearing temperature > Max2 (i=1 to 4)	SAS	SPPA-T2000
Reactor coolant pump i motor upper pad temperature > Max2 (i=1 to 4)	SAS	SPPA-T2000
Reactor coolant pump i motor lower bearing temperature > Max2 (i=1 to 4)	SAS	SPPA-T2000
Reactor coolant pump i motor lower pad temperature > Max2 (i=1 to 4)	SAS	SPPA-T2000
Standstill Seal System i (SSSS) actuation (i=1 to 4)	SAS	SPPA-T2000
10kV LHi voltage < Min1 (i=A to D)	PS (Sub-S. A) PS (Sub-S. B)	TXS

Signal description	I&C system	Technology
Hot leg pressure < Min2 WR	SAS	SPPA-T2000
SGi level < Min3 WR (i=1 to 4)	SAS	SPPA-T2000
Hot leg pressure < Min1 WR	PS (Sub-S. B)	TXS
Hot leg pressure < Min3 WR	SAS	SPPA-T2000
Diversified signal reactor primary coolant loop level < Min1	SAS	SPPA-T2000
Reactor Trip check-back	PS (Sub-S. A) PS (Sub-S. B)	TXS
Safety Injection for Partial Cooldown train i (i=1 to 4)	PS (Sub-S. B)	TXS
Flow rate downstream ASG [EFWS] pump i (i=1 to 4)	PS (Sub-S. A)	TXS
Antidilution signal - states B to Ca	PS (Sub-S. B)	TXS
Antidilution signal - states Cb to D	PS (Sub-S. B)	TXS
Reactor coolant pump i trip (seal injection + thermal barrier) (i=1 to 4)	SAS	SPPA-T2000
RRI [CWCS] tank i level < Min3 (i= 1 to 4)	SAS	SPPA-T2000
Very low level in the Volume Control Tank (level < Min5)	SAS	SPPA-T2000
Normal switchover of RCV [CVCS] pumps	SAS	SPPA-T2000
Average coolant temperature control	RCSL	TXS
Antidilution - states B to Ca	RCSL	TXS
Emergency Diesel Generator (EDG) train i reloaded sequence after LOOP (i= 1 to 4)	PS (Sub-S. A) PS (Sub-S. B)	TXS
Main Feedwater Pumps off	Not processed by PS[1]	
High RPE sump pressure outside containment LHSI train 1	PS (Sub-S. A)	TXS
Alarm "Low Fuel Pool Cooling System flow rate" train i (i=1 to 2)	SAS	SPPA-T2000
Neutron flux (power range) > MAX1N	NCSS	Hardwire
SGi level > MAX1N (i=1 to 4)	NCSS	Hardwire
SGi pressure > MAX1N (i=1 to 4)	NCSS	Hardwire
SGi level < MIN1N (i=1 to 4)	NCSS	Hardwire
Hot leg pressure < MIN1N	NCSS	Hardwire
Hot leg pressure > MAX1N	NCSS	Hardwire
Main Feedwater isolation on SGi level > MAX2N (i=1 to 4)	NCSS	Hardwire
Seal leak-off line isolation on Reactor Coolant Pump i seal cavity temperature > MAX1N (i=1 to 4)	NCSS	Hardwire
Reactor Coolant Pump i trip (i=1 to 4)	NCSS	Hardwire
RCV [CVCS] letdown line isolation on Reactor Primary Coolant level < MIN1N	NCSS	Hardwire
ASG [EFWS] train i start-up on SGi level < MIN2N	NCSS	Hardwire
Switchover to DEL [SCWS] cooling on LHSI train i (i= 1 and 4)	SAS	SPPA-T2000
MONITORING SIGNALS		
Alarm "Low discharge pressure" (FPCS pump - train i) (i =1 to 2)	SAS	SPPA-T2000

[1] To be updated when detailed design of SSS [AAD] is available.

Signal description	I&C system	Technology
Alarm "High temperature of Spent Fuel Pool"	SAS	SPPA-T2000
Indication of high Spent Fuel Pool temperature	NCSS	Hardwire
Indication of Core Outlet Temperature (OSSA entering criteria)	NCSS	Hardwire
Indication of Core Outlet Temperature (OSSA entering criteria)	SA I&C	TXS
Indication of high neutron flux power range	NCSS	Hardwire

SECTION 15.1.3 - TABLE 4

Probability of failure of a post-accident task

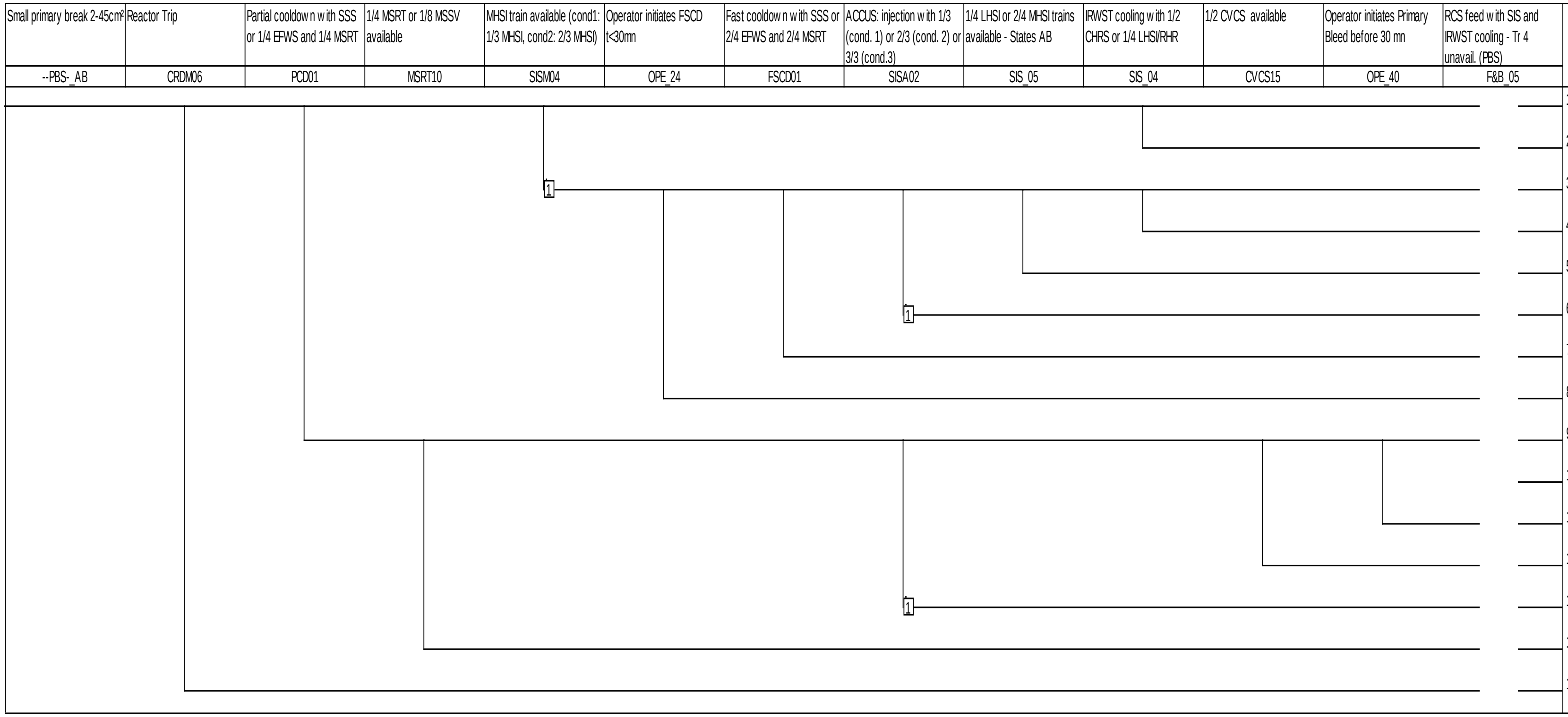
				P (5)	
T_m (min) (1)	**T_d (min)** (2)	**P_d** (3)	**P_{NRa}** (4)	**P_a = 0.05** (6)	**P_a = 0.25** (6)
5	0	1.0E+00	1	1.00E+00	1.00E+00
10	5	6.2E-01	1	6.35E-01	7.12E-01
15	10	5.0E-01	1	5.25E-01	6.25E-01
20	15	2.0E-01	1	2.35E-01	3.96E-01
25	20	1.0E-01	1	1.45E-01	3.25E-01
30	25	2.8E-02	0.3	4.28E-02	1.01E-01
35	30	1.0E-02	0.3	2.49E-02	8.43E-02
40	35	6.0E-03	0.3	2.09E-02	8.05E-02
45	40	3.9E-03	0.3	1.88E-02	7.86E-02
50	45	2.6E-03	0.3	1.76E-02	7.74E-02
55	50	1.8E-03	0.3	1.68E-02	7.67E-02
60	55	1.3E-03	0.03	2.84E-03	8.83E-03
65	60	1.0E-03	0.03	2.50E-03	8.49E-03
70	65	9.4E-04	0.03	2.44E-03	8.44E-03
80	75	8.5E-04	0.03	2.35E-03	8.35E-03
90	85	7.8E-04	0.03	2.28E-03	8.27E-03
120	115	6.3E-04	0.03	2.13E-03	8.12E-03
150	145	5.3E-04	0.03	2.03E-03	8.03E-03
180	175	4.6E-04	0.03	1.96E-03	7.96E-03
210	205	4.1E-04	0.03	1.91E-03	7.91E-03
240	235	3.7E-04	0.03	1.87E-03	7.87E-03
> 240 (7)	> 235	1.0E-04	0	1.0E-04	1.0E-04

{CCI removed}

a

SECTION 15.1.3 – FIGURE 1

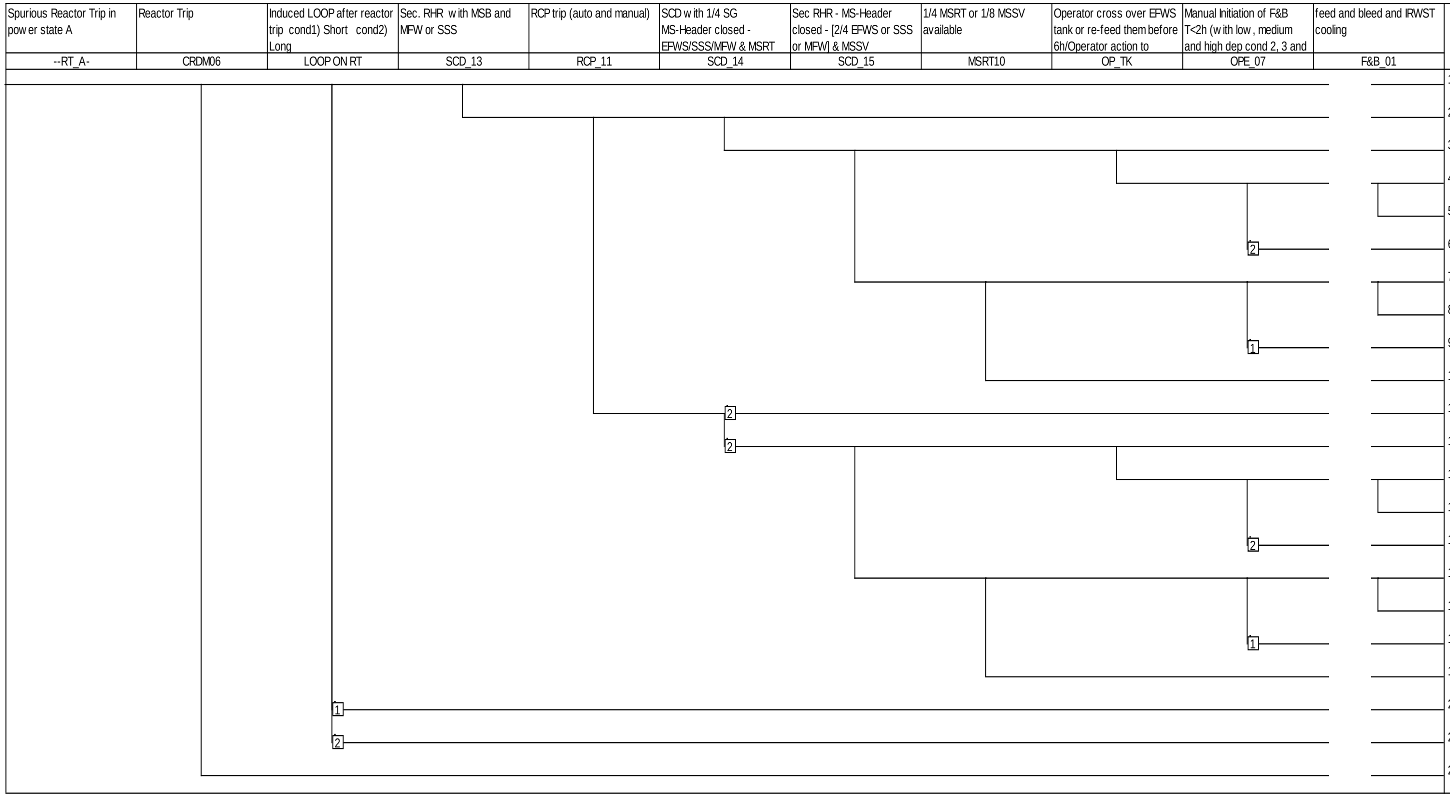
Event Tree - Small LOCA [2 – 45 cm²] in at-power state A and intermediate shutdown state B


Small primary break 2-45cm²
--PBS-_AB
Reactor Trip
CRDM06
Partial cooldow n w ith SSS or 1/4 EFWS and 1/4 MSRT
PCD01
1/4 MSRT or 1/8 MSSV available
MSRT10
MHSI train available (cond1: 1/3 MHSI, cond2: 2/3 MHSI)
SISM04
Operator initiates FSCD t<30mn
OPE_24
Fast cooldow n w ith SSS or 2/4 EFWS and 2/4 MSRT
FSCD01
ACCUS: injection w ith 1/3 (cond. 1) or 2/3 (cond. 2) or 3/3 (cond.3)
SISA02
1/4 LHSI or 2/4 MHSI trains available - States AB
SIS_05
IRWST cooling w ith 1/2 CHRS or 1/4 LHSI/RHR
SIS_04
1/2 CVCS available
CVCS15
Operator initiates Primary Bleed before 30 mn
OPE_40
RCS feed w ith SIS and IRWST cooling - Tr 4 unavail. (PBS)
F&B_05
1
1
1

No.	Freq.	Conseq.	Code
1	1,18E-03	L, S	
2	2,72E-11	F, SL	SIS_04
3	1,54E-07	LF, S	SISM04
4	3,15E-12	F, SLD	SISM04-SIS_04
5	1,91E-10	F, SLD	SISM04-SIS_05
6	1,65E-13	F, SLD	SISM04-SISA02
7	3,66E-10	F, SLD	SISM04-FSCD01
8	4,60E-08	F, SL	SISM04-OPE_24
9	2,77E-08	LF, S	PCD01
10	2,13E-10	F, SL	PCD01-F&B_05
11	5,84E-09	F, SL	PCD01-OPE_40
12	4,07E-11	F, SL	PCD01-CVCS15
13		F, SL	PCD01-SISA02
14	1,03E-14	F, SL	PCD01-MSRT10
15	1,18E-03	ATWS	CRDM06

SECTION 15.1.3 – FIGURE 2

Event Tree - Reactor Trip in at-power state A

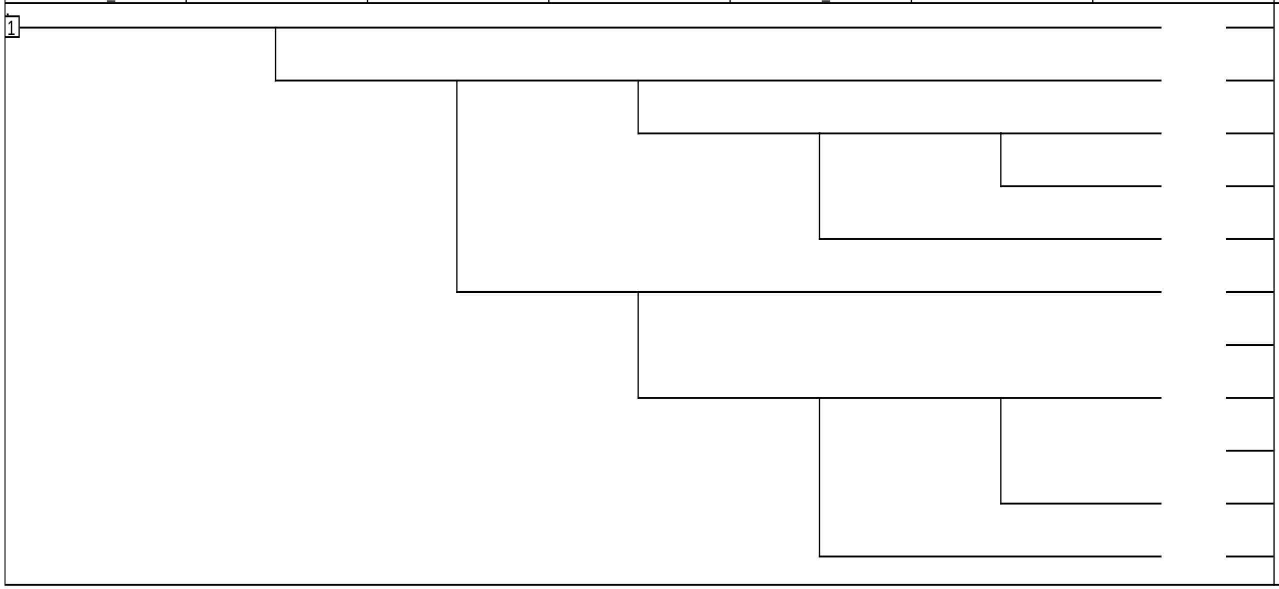

Spurious Reactor Trip in pow er state A
--RT_A-
Reactor Trip
CRDM06
Induced LOOP after reactor trip cond1) Short cond2) Long
LOOP ON RT
Sec. RHR w ith MSB and MFW or SSS
SCD_13
RCP trip (auto and manual)
RCP_11
SCD w ith 1/4 SG MS-Header closed - EFWS/SSS/MFW & MSRT
SCD_14
Sec RHR - MS-Header closed - [2/4 EFWS or SSS or MFW] & MSSV
SCD_15
1/4 MSRT or 1/8 MSSV available
MSRT10
Operator cross over EFWS tank or re-feed them before 6h/Operator action to
OP_TK
Manual Initiation of F&B T<2h (w ith low , medium and high dep cond 2, 3 and
OPE_07
feed and bleed and IRWST cooling
F&B_01
2
1
2
2
2
1
1
2

No.	Freq.	Conseq.	Code
1	1,00E+00	S, T	
2	1,00E-01	S, T	SCD_13
3	1,48E-05	S, T	SCD_13-SCD_14
4	1,47E-09	LF, S	SCD_13-SCD_14-OP_TK
5	2,02E-12	F, TR	SCD_13-SCD_14-OP_TK-F&B_01
6	3,72E-10	F, TR	SCD_13-SCD_14-OP_TK-OPE_07
7	1,29E-08	LF, S	SCD_13-SCD_14-SCD_15
8	7,95E-12	F, TR	SCD_13-SCD_14-SCD_15-F&B_01
9	1,05E-10	F, TR	SCD_13-SCD_14-SCD_15-OPE_07
10	1,56E-11	F, TR	SCD_13-SCD_14-SCD_15-MSRT10
11	1,50E-07	S, T	SCD_13-RCP_11
12	2,40E-09	S, T	SCD_13-RCP_11-SCD_14
13	2,37E-13	LF, S	SCD_13-RCP_11-SCD_14-OP_TK
14	5,09E-12	F, TR	SCD_13-RCP_11-SCD_14-OP_TK-F&B_01
15	1,54E-11	F, TR	SCD_13-RCP_11-SCD_14-OP_TK-OPE_07
16	2,89E-13	LF, S	SCD_13-RCP_11-SCD_14-SCD_15
17	1,67E-11	F, TR	SCD_13-RCP_11-SCD_14-SCD_15-F&B_01
18	1,00E-09	F, TR	SCD_13-RCP_11-SCD_14-SCD_15-OPE_07
19	6,48E-13	F, TR	SCD_13-RCP_11-SCD_14-SCD_15-MSRT10
20	3,33E-04	LOOPS AB	LOOP ON RT
21	6,67E-04	LOOPL AB	LOOP ON RT(3)
22	1,00E+00	ATWS	CRDM06

SECTION 15.1.3 – FIGURE 3

Event Tree - Uncontrolled Level Drop during shutdown state D

Uncontr. Level Drop	automatic closure of purification and letdown line from PS (and RCSL)	Automatic CVCS isolation from SAS	1/4 MHSI train avail. state CB-E (cond. 1) or state Ca (cond. 2)	Operator starts SIS t=20'	1/4 LHSI available for safety injection	Manual isolation of letdown line
--ULD--_D-	CVCS12	CVCS14	SISM06	OPE_47	SISL43	CVCS11



No.	Freq.	Conseq.	Code
1	8,05E-06	S, V1	
2	1,69E-09	S, V1	CVCS12
3	9,14E-14	S, V1	CVCS12-SISM06
4	1,38E-13	F, TR (D)	CVCS12-SISM06-SISL43
5	1,80E-11	F, TR (D)	CVCS12-SISM06-OPE_47
6	6,84E-13	S, V2	CVCS12-CVCS14
7		F, TR (D)	CVCS12-CVCS14-CVCS11
8	2,03E-12	S, V2	CVCS12-CVCS14-SISM06
9		F, TR (D)	CVCS12-CVCS14-SISM06-CVCS11
10		F, TR (D)	CVCS12-CVCS14-SISM06-SISL43
11	2,45E-13	F, TR (D)	CVCS12-CVCS14-SISM06-OPE_47

4. INTERNAL INITIATING EVENTS

This section presents and discusses the internal initiating events analysed in the PSA and presents the sequence frequencies derived using the Level 1 PSA.

An initiating event is an event which creates a disturbance in the plant and has the potential to lead to core damage, depending on the successful operation of the various mitigating systems in the plant. The initiating event can be an internal or external event e.g. a component failure, a natural phenomenon or a human caused hazard.

Initiating events may result in a disturbance in the balance between heat production in the core, or the fuel pool, and the associated heat removal such that countermeasures are required to prevent core or fuel damage.

4.1. SCOPE

An initiating event is an event that creates a disturbance in the plant and has the potential to lead to Core Damage. The outcome of the event is dependent on the operation of the various plant mitigating systems.

A summary of the Initiating Events analysed in the PSA with their frequencies is presented in Section 15.1.4 - Table 4. A discussion of the initiating events is carried out group by group.

The list of initiating events will be updated during the site-specific assessment phase of the UK EPR as the number of events that need to be modelled in the PSA will be increased.

The initiating events considered in the PSA described in this sub-chapter are limited to internal events. Initiating events related to internal and external hazards are discussed in Sub-chapter 15.2.

The selection of initiating events to be modelled in a PSA is the first crucial step in the development of a plant PSA model. Before defining and analysing the event sequences, the identified initiating events must first be divided into suitable groups with similar characteristics [Ref-1].

The following methods and sources have been used to ensure a systematic and exhaustive search for potential initiating events [Ref-1]. This is consistent with the approach discussed in IAEA-TECDOC-719 [Ref-2]:

- Engineering evaluation or technical study of the plant (see Chapter 14, Design Basis Analysis),

- Previous PSAs such as the supporting document for FA3 PSAR Chapter 18.1 [Ref-3], the Basic Design Report [Ref-4] or French 1300 MWe [Ref-5] and 900 MWe [Ref-6] PSA,

- Lists of initiating events such as NUREG/CR-3862 [Ref-7], NUREG/CR-6928 [Ref-8] and NUREG-1829 [Ref-9],

- Analysis of operating experience for actual plant discussed in FA3 PSAR Chapter 18.1 [Ref-10],

- FMEA (Failure Modes and Effects Analysis) of EPR systems.

The aim of the grouping of initiating events is to develop a set of initiating events which meets the following key attributes [Ref-1]:

1. The set must cover all plant relevant initiating events.
2. The set must be defined in sufficient detail to ensure that all of the safety functions and their associated systems can be examined in the event trees in the appropriate sequence. It must also ensure that the important dependencies between the initiating events and the safety systems can be evaluated.
3. The set must include the initiating events that make the highest demands on safety systems.

The UK EPR PSA splits the LOCA and transients categories into several fault groups as listed below:

- **Loss of primary coolant accident (LOCA)**. This fault group includes all faults leading to the loss of the secondary barrier to radiological release, the RCP [RCS];
- **Primary system transients**: This fault group includes faults directly affecting the physical parameters of the RCP [RCS];
- **Loss of off-site power (LOOP)**: Generally, this type of transient is treated separately from primary and secondary transients due to its specific impact on all plant systems;
- **Secondary system break**: This fault group includes secondary pipe breaks that affect the heat removed by the secondary side;
- **Secondary system transients**: This fault group includes faults in systems involved in the secondary side heat removal;
- **Loss of cooling water systems**: This fault group includes faults on systems belonging to the main cooling chain RRI/SEC [CCWS/ESWS];
- **Transient without automatic reactor shutdown (ATWS)**: This fault group includes faults affecting the control of the reactivity function in transients requiring a reactor trip.

The initiating events involved in the different fault groups are identified below.

4.1.1. Initiating events during full and low power operation (standard reactor states A & B)

- Loss of primary coolant accident (LOCA):
  - 2A-LOCA
  - Large break [180 – 830 cm²]
  - Medium break [45 – 180 cm²]
  - Small break [2 – 45 cm²]

  - Interfacing system LOCA (Containment bypass)
  - Steam generator tubes rupture (SGTR) of 1 or 2 tubes
  - Reactor Pressure Vessel failure
- Primary system transients
  - Spurious reactor trip
  - Homogeneous boron dilution,
  - Heterogeneous boron dilution
- Loss of off-site power (LOOP):
  - Total loss of off-site power (0 - 2 hours)
  - Total loss of off-site power (2 - 24 hours)
- Secondary system break:
  - Large secondary side breaks inside the containment
  - Large steam line breaks outside containment, downstream of the Main Steam Isolation Valves
  - Small break on secondary side
  - Steam line break inducing SGTR
- Secondary system transients:
  - Total loss of main feedwater
  - Loss of the start-up and shutdown feed system
  - Loss of condenser
  - Turbine trip
- Loss of cooling water systems:
  - Partial or total loss of the cooling chain
- Transient without automatic reactor shutdown (ATWS)

4.1.2. Initiating events during shutdown operation (standard reactor states C, D and E)

- Loss of primary coolant accident
  - Small break [2 – 20 cm^2]

- Interfacing system LOCA (Containment bypass)

- Loss of off-site power (LOOP)
  - Total loss of off-site power (0 - 2 hours)
  - Total loss of off-site power (2 - 24 hours)
- Primary system transients:
  - Homogeneous boron dilution
  - Heterogeneous boron dilution
  - Total loss of RIS-RRA [SIS-RHR] in shutdown states
  - Uncontrolled drop in primary coolant level
- Loss of cooling water systems:
  - Total loss of the cooling chain

4.1.3. Quantification of the frequency of initiating events

The frequencies of initiating events are evaluated from:

- French or international operational experience feedback [Ref-1] to [Ref-5],
- Calculations of the failure probability of specific equipment, e.g. loss of cooling systems, using the component reliability database [Ref-6].

The quantification method depends on the initiating event group.

- For initiating events that have already occurred:
  - 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);
  - For frequent initiating events (i.e. those observed at least once in French plants), the operational experience of the 1300 MWe PWR series is preferred. This may be augmented on a case by case basis by operational experience from French 900 MW stations.
- For initiating events not observed in French or international operational experience, the frequency may be evaluated in two ways:
  - The χ^2 method at 50% at two degrees of freedom: The estimate of the frequency is calculated as the upper bound of the one-sided confidence interval at the 50% confidence level. The actual frequency has an equal probability of being higher or lower than the estimated value. Therefore:

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

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

Generally, the systematic use of the χ^2 method at 50% is avoided. This is because the χ^2 method at 50% leads to clustering of the frequencies of all hypothetical initiating events around just two values. This homogenisation is counter-intuitive and conflicts with the PSA objective, which is to rank sequences leading to core damage. As far as possible, expert judgement is preferred for initiating events which have not occurred at a nuclear site.

- For initiating events resulting from component failure, the frequency is calculated from reliability data for the relevant component.

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

4.2. LOSS OF PRIMARY COOLANT ACCIDENTS (LOCA)

4.2.1. Primary breaks

The primary break spectrum is defined to be consistent with the results of thermal-hydraulic analysis performed to support the EPR PSA. It is concluded that:

- 2A-LOCA event, the failure rate assumed in the PSA is {CCI removed} a according to the quality assurance processes followed in the manufacturing and in the control of welds. This frequency is consistent with §244 of the HSE SAPs [Ref-1]. It is stated in the SAPs that […] "As a general guide, claims for pipework weld failure rates for gross failure (e.g. guillotine failure) much better than 1 x 10-8 to 1 x 10-9 per weld year should not be considered.".

There are 9 girth welds per RCP [RCS] loop, as discussed in Sub-chapter 5.2:

- 4 connections vessel / hot-leg
- 4 connection hot leg / steam generator
- 4 connection Steam generator / U-leg
- 4 connection U-leg / Reactor coolant pump
- 4 connection reactor coolant pump /cold-leg
- 4 connection cold-leg / vessel
- 4 connections cold-leg / safety injection (RIS)
- 4 connections hot-leg / residual heat removal (RHR)

- o 2 connections cold-leg / RCV [CVCS] injection – loops 2 and 4
- o 1 connection U-leg / RCV [CVCS] discharge – loop 1
- o 1 connection hot-leg / pressuriser – loop 3

However, the large LOCA initiating event frequency considers a rupture with a break area between 180 cm² and 830 cm². The largest break considered is the rupture of the Pressuriser surge line, see below. The failure of the following welds is considered in the Large LOCA and has not to be considered in the 2A-LOCA:

- o 4 connections cold-leg / safety injection (RIS)
- o 4 connections hot-leg / residual heat removal (RHR)
- o 2 connections cold-leg / RCV [CVCS] injection – loops 2 and 4
- o 1 connection U-leg / RCV [CVCS] discharge – loop 1
- o 1 connection hot-leg / pressuriser – loop 3

Thus, the 2A-LOCA on the RCP [RCS] system has a frequency of:

{CCI removed} [a]

This frequency is conservative compared to the frequency presented in NUREG-1829 [Ref-2].

- <u>Large primary breaks (PBL1) between 180 cm² and 830 cm².</u> The largest break considered is the rupture of the pressuriser surge line. This size of break leads to a rapid and significant depressurisation of the primary side down to the Low Head Safety Injection (LHSI) pressure. No secondary cooldown or primary bleed is required to reach the Safety Injection pressure threshold.

- <u>Medium primary breaks (PBM) are between 45 cm² and 180 cm².</u> This group is divided into two sub-categories:

    - o <u>Medium/Large (PBM1) between 100 cm² and 180 cm².</u> This size of break is sufficient to depressurise the primary side to the MHSI injection pressure without secondary partial cooldown.

    - o <u>Medium/small (PBM2) between 45 cm² and 100 cm²</u>. This size of the break is sufficient to depressurise the primary side to the MHSI injection pressure. Secondary partial cooldown is not required but is assumed in the PSA to improve the MHSI success criteria.

- <u>Small primary breaks (PBS) during power operation, between 2 cm² and 45 cm².</u> The break size is too large to be compensated by the RCV [CVCS]. The break is not sufficiently large to ensure depressurisation of the primary circuit to the Medium Head Safety Injection (MHSI) injection pressure. A partial secondary cooldown is required to reach the MHSI pressure.

For shutdown states (Ca, Cb, D and E), the break size studied is between 2 cm² and 20 cm². Due to the lack of data for small LOCA events in shutdown states, the small break LOCA frequencies in shutdown states are derived from the small LOCA frequencies in at-power states (NUREG-6928 [Ref-3]). This is considered conservative as mechanical stresses are significantly lower in shutdown states due to low reactor coolant system pressure and temperature. Breaks larger than 20 cm² as a result of mechanical rupture induced by pressure, wear, corrosion or thermal fatigue, are not considered when the RCP [RCS] pressure and temperature are at shutdown conditions.

Note: In shutdown states the potential rupture of an LHSI/RHR suction line (490 cm²) is considered as an interfacing system LOCA event (see sub-section 4.3 of this sub-chapter).

- A pressuriser leak is considered as a spurious opening and failure to close of a pressuriser safety valve. The pressuriser leak is equivalent to a small primary break (PBS). Plant behaviour following a stuck open pressuriser safety valve is similar to that in the case of a PBS. The frequency of a pressuriser leak in shutdown state Ca is assessed from the period of operation in state Ca per year.

In at-power state A or intermediate shutdown state B, the primary break frequencies are obtained from:

- NUREG/CR-6928 [Ref-3] for small and large break frequencies,
- NUREG-1829 [Ref-2] for small (in addition to NUREG-6928 [Ref-3]) and medium break frequencies and
- Specific reliability analysis and operating experience feedback has been considered in deriving the pressuriser leak frequency [Ref-4].

The primary break frequencies considered in the PSA are as follows:

- PBL-2A_AB = {CCI} [a]
- PBL1_AB = 1.3E-06/y
- PBM2_AB (45-100 cm2) + PBM1_AB (100-180 cm^2) = 8E-06 + 8E-06 = 1.6E-05/y. It is conservatively assumed that 50% of the breaks can be allocated to the PBM1 range (8E-06/y) and 50% to the PBM2 range (8E-06/y). This leads to the overestimation of the PBM1 break range, which has the higher conditional core damage probability.
- PBS_AB (2-20 cm²) + PBS_AB (20-45 cm²) = 5.77E-04 + 6.04E-04 = 1.18E-03/y
- PZR leak AB = {CCI} [a]

In shutdown states Ca, Cb, D and E the assumed initiating event frequencies are:

- PBS_CA = 3.9E-06/y
- PZR leak_CA = {CCI} [a]
- PBS_CB = 5.5E-06/y

- PBS_D = 3.0E-06/y
- PBS_E = 8.3E-06/y

4.2.2. Reactor Pressure Vessel Failure

The EPR vessel factory follows the latest manufacturing technology which incorporates the operating experience of the existing PWR fleet. In addition, the EPR is designed to prevent pressure transients which could challenge the vessel integrity. It is considered that the risk of RPV failure is extremely low and a frequency of {CCI} [a] is assumed in the level 1 PSA. This frequency is consistent with the SAPs [Ref-1], §244 which states "[…] *a claim that gross failure of a pressure vessel can be discounted cannot plausibly be associated with a failure rate much better than 1x10^{-7} to 1x10^{-8} per vessel year".*

In the PSA it is assumed that the failure of the RPV leads directly to core damage.

4.2.3. Interfacing system LOCA (V-LOCA)

Interfacing system LOCAs are analysed in the Level 1 PSA. A V-LOCA is a break in a system connected to the Reactor Coolant System (RCP [RCS]), and partly located outside containment. This type of break may lead to a loss of coolant accident and draining of the IRWST outside the containment if the break is not isolated. This type of transient involves a containment bypass via auxiliary systems connected to the reactor coolant system.

In at-power states A and B, the study reported in EPSE DC 833 [Ref-1] concludes that the failure probability of the levels of defence challenged by V-LOCA initiating events is very low at {CCI} [a]. It is conservatively assumed in the Level 1 PSA that an unisolated V-LOCA in at-power states A and B would lead directly to core damage. The V-LOCA initiating events considered in the analysis are listed in Section 15.1.4 - Table 1.

The frequencies for V-LOCA scenarios in the Residual Heat Removal System (RRA [RHRS]) when it is connected to the primary circuit in shutdown states Ca, Cb, D and E are obtained from the German safety analysis of NPP [Ref-2]. The initiating events studied are:

- A small external break (5 – 20 cm²) in the RRA [RHRS] in states C to E which have the following frequencies:

{CCI removed}

a

- A significant external break (>20 cm² and breaks of a diameter equal to DN250 (size of LHSI/RHR lines) in the RRA [RHRS] in states C to E which have the following frequencies:

{CCI removed}

{CCI removed} [a]

- The frequency of the rupture of two tubes in an RRA [RHRS] heat exchanger in state C without isolation is {CCI} [a] (by fault tree analysis). This initiating event is therefore not considered in the UK EPR PSA due to its low frequency.

4.2.4. Steam Generator Tube(s) Rupture (SGTR)

This family of events includes the rupture of one or two steam generator tubes. These initiating events can result in a bypass of the containment if the isolation of the affected steam generator fails. Primary coolant can then be lost outside the containment leading to a radioactivity release even if core damage is avoided.

The rupture of more than two tubes is not analysed. The frequency of such an event is assumed to be negligible.

The frequencies, taken from EDF analysis performed for EPR [Ref-1], are:

- 1 Steam Generator Tube Rupture: SGTR1_AB = {CCI} [a]
- 2 Steam Generator Tube Ruptures: SGTR2_AB = {CCI} [a]

4.3. SECONDARY SYSTEM BREAKS (SLB)

Secondary System Break initiating events include breaks in the secondary system (steam or feed water) and Steam Generator Tube Ruptures induced by a secondary system break.

4.3.1. Breaks in Secondary System (steam or feed water)

- Large secondary side breaks inside the containment (SLB_LI_AB). These include large steam line breaks inside the containment, and large feedwater line breaks, located between the last feedwater line check valve and the SG.

  The consequences of a feedwater line break inside the containment are covered by those of steam line breaks. The release of steam within the containment following a feedwater line break is less significant. In addition, the feedwater line length is shorter than steam line. For other aspects, the response of the plant to the two faults is similar.

  The frequency of a main steam line break inside the containment is similar to the frequency of a large LOCA (PBL1). This is reasonable as the quality of production of the main steam line is similar to that of the primary loops, and the break preclusion principle applies equally to both types of pipe.

  The frequency, taken from NUREG/CR-6928 [Ref-1], is: SLB_LI_AB = 1.3E-06/y.

- Large steam line breaks downstream of the Main Steam Isolation Valves (SLB_LO_AB). These include large steam line breaks located downstream of the MSIV, and main feedwater line breaks downstream of the feedwater isolation valves, or any initiating events leading to the same consequences.

The frequency, taken from EDF supporting document [Ref-2], is: SLB_LO_AB = {CCI} [a].

- Small steam line un-isolatable breaks (SLB_SO_AB). These include un-isolatable small steam line breaks or equivalent initiators caused by secondary-side transients, and small feedwater line breaks inside the containment, located between the last feedwater line check valve and the SG. They include spurious opening of a Main Steam Relief Isolation Valve (VDA [MSRT]) and a stuck open Main Steam Safety Relief Valve (VVP [MSSS]).

The frequency, from EDF supporting document [Ref-2], is: SLB_SO_AB = {CCI} [a].

In secondary system transients such as a loss of condenser or turbine trip, with MSIV closure, the secondary overpressure protection devices (VDA [MSRTs] or VVP [MSSVs]) are challenged. This is discussed further in sub-section 5.6 of this sub-chapter.

- If a VDA [MSRT] or VVP [MSSV] fails to close after their actuation, a small steam line break should be assumed. The probability of this event is assessed at {CCI} [a] (by fault tree analysis). The frequency of the MSIV closure should not exceed 1/y. Therefore the assumed small steam line break frequency (SLB_SO_AB) covers this initiating event.
- If the VDA [MSRT] or the VVP [MSSVs] fail to open following closure of 1 MSIV, a large steam line break is assumed. The frequency of MSIV closure is F = {CCI} [a] according to EDF supporting document [Ref-2]. The probability of failure of the protection against this event is assessed at {CCI} [a] (by fault tree). Therefore the frequency of a large steam line break assumed in the PSA covers this type of initiating event.

4.3.2. Secondary Breaks and SGTR

This type of transient could occur following a significant depressurisation of the steam generator. The integrity of the steam generator tubes could be challenged by a significant pressure differential between the secondary and the primary sides. For each secondary side break presented in sub-section 4.5.1 of this sub-chapter, it is assumed that consequential rupture of no more than two steam generator tubes could occur. The following conditional probabilities of SGTR, following a steam line break, have been taken from EDF supporting document [Ref-1], following discussions between EDF and IRSN:

- {CCI} [a] in case of Large Steam Line Break inside or outside the containment.
- {CCI} [a] in case of small Steam Line Break outside the containment.

Comparison of these values with the conditional probabilities proposed in NUREG/CR-6365 [Ref-2] proves their applicability.

The frequencies of the three transients studied are thus:

- SLB_LI_SGTR_AB = {CCI} [a],
- SLB_LO_SGTR_AB = {CCI} [a],

- SLB_SO_SGTR_AB = {CCI} [a].

4.4. SECONDARY SYSTEM TRANSIENTS

These transients are characterised by a perturbation of the normal steam generator feedwater (ARE) [MFWS] flow leading to a reactor trip. This group includes the following initiating events:

4.4.1. Total Loss of Main Feedwater (LOMFW_A)

Total Loss of Main Feedwater during power operation – LOMFW_A is assumed to follow a malfunction of the ARE [MFWS] resulting in a decrease in the normal SG feedwater flow during power operation (State A).

The Loss of Main Feedwater (LOMFW) frequency in State A is taken from operating experience on French 1300 MWe PWRs. {CCI removed} [a] according to formula given in section 4.1.3.

4.4.2. Total Loss of Start-up and Shutdown feed System (AAD) [SSS] (LOSSS_B)

Total Loss of the Start-up and Shutdown feed System (AAD) [SSS] is assumed to occur during intermediate shutdown (state B). This transient follows the malfunction of the AAD [SSS], in service in place of the ARE [MFWS] following reactor shutdown. This transient does not lead to a reactor trip as the reactor is already tripped in plant state B.

The frequency of this transient derived from fault tree analysis is LOSSS_B = {CCI} [a].

4.4.3. Spurious Turbine Trip (TT_A)

Spurious Turbine Trip during power operation – TT_A - is characterised by the loss of secondary load due to the turbine trip, and the opening of the Main Steam Bypass valves (GCT) [MSB]. A loss of load event generates a partial trip to ~50% power quickly enough to avoid a high power trip. A partial trip with the GCT [MSB] to the condenser actuated, allows the plant to quickly return to full power. This intermediate state is not currently included in the PSA model.

The frequency, taken from EDF supporting document [Ref-1], is: TT_A = {CCI} [a].

4.4.4. Loss of condenser (LOC_AB)

Loss of condenser during power operation – LOC_AB - covers the loss of condenser vacuum event, the loss of circulating pumps (CEX) and the spurious closure of all MSIVs. The GCT [MSB] is assumed to be unavailable following the initiating event. The consequences to the plant are similar to those following a turbine trip.

The frequencies of the initiating events considered are the following:

- Loss of condenser vacuum, derived from the EUR [Ref-1]: F=1.0E-01/y
- Loss of Circulating pumps, derived from the EUR [Ref-1]: F=5.0E-02/y

4.5. LOSS OF ELECTRICAL SUPPLY

The Loss of electrical supply studied in the PSA corresponds to the loss of offsite power initiating event (LOOP). The loss of high or medium voltage panels events are not analysed at this stage of the analysis.

4.5.1. LOOP during Power Operation (states A and B)

The frequencies as derived from the EUR [Ref-1] are as follows:

LOOPS_AB = 6E-02/y.

- Short LOOP corresponds to the most frequent grid failures, with a short recovery time (< 2 hours).

LOOPL_AB = 1E-03/y.

- long LOOP events are due to less frequent grid faults between the plant and the transformer and by line faults due to severe weather in the vicinity of the plant.

The loss of offsite power initiating event (LOOP) is defined as a complete loss of the main and auxiliary grid. Switchover to the main generator (house load operation) is also assumed to fail as the PSA does not claim this potential success state.

LOOP results in all systems that depend on normal AC power being lost. This includes the reactor coolant pumps, the Main Feedwater System (ARE [MFWS]), the Main Steam Bypass (GCT [MSB]), and the Start-up and Shutdown System (AAD [SSS]). This initiating event also demands operation of the emergency diesel generators to supply AC power to all four safety system divisions. The diesels are automatically started following detection of a LOOP. Subsequently, restart of any normal operating equipment, e.g. Component Cooling Water System, Essential Service Water System and Chemical and Volume Control System, is required. LOOP is also one of the most likely challenges to reactor coolant pump seal cooling, and consequential seal failure due to LOOP is included in the model.

As offsite power is readily recoverable, the possibility of recovering offsite power is assessed to ensure a realistic analysis of the plant response. Two types of LOOP are studied:

- Short duration LOOP, lasting less than two hours – LOOPS: The main or auxiliary grid is assumed to be recovered within two hours. The plant can reliably operate for at least two hours without any AC power. The inventory in the steam generators will last 90 minutes and the time to core uncovery is longer than 2 hours. In addition, the batteries will not be fully depleted in two hours.

  The frequency derived from the EUR [Ref-1] is: LOOPS_AB = 6.0E-02/y.

  Operational evidence [Ref-2] shows that short LOOP corresponds to the most frequent grid failures, with a short recovery time.

- Long LOOP lasting less than 24 hours - LOOPL. The main grid is recovered within 24 hours. In the LOOP fault sequence model, if offsite power is not recovered within a two-hour period, a successful plant response requires a stable state to be maintained for the full 24 hour mission time. In the event of failure of the four Emergency Diesels Generators, two station blackout (SBO) diesels are available, which can be manually aligned by the operators within the two-hour time window available.

  The SBO diesels can supply two ASG [EFWS] pumps, the necessary I&C and ventilation. In addition, two LHSI pumps or two EVU [CHRS] trains and their dedicated cooling water can be supplied.

  The frequency derived from the EUR [Ref-1] is: LOOPL_AB = 1.0E-03/y.

  Operational evidence [Ref-2] shows that long LOOP events arise mainly due to grid faults between the plant and the transformer and line faults caused by severe weather in the vicinity of the plant.

4.5.2. LOOP during shutdown states (states Ca, Cb, D and E)

The loss of offsite power initiating event (LOOP) is defined as a complete loss of the main and auxiliary grid. LOOP results in the loss of all systems that depend on normal AC power.

The LOOP initiating event requires operation of the emergency diesel generators to supply AC power to the four safety system divisions. The diesels are automatically started following detection of a LOOP. Subsequently, restart of any normal operating equipment is required. In particular Residual Heat Removal Trains in operation before the LOOP are required to be automatically restarted.

As offsite power is readily recoverable, the probability of recovering offsite power is taken into account to ensure a realistic analysis of the plant response. Two types of LOOP are studied:

- Short LOOP, lasting less than two hours – LOOPS: The main grid is recovered within two hours. The plant can reliably operate for at least two hours without AC power (SBO).

  In state Ca and Cb, if the main diesels do not start (SBO), heat removal is provided by the inventory in the steam generators which will last much longer than two hours The time to core uncovery in these circumstances is significantly longer than two hours. However failure of the batteries after two hours will result in the closure of the Main Steam Relief Train and interruption of the residual heat removal via the SGs. If the grid is recovered before the failure of the batteries (i.e. LOOP 2 hours), the electrical supply from batteries is sufficient to mitigate the accident.

  In state D, the water inventory in the primary circuit is very low and the secondary side is unavailable. Makeup via the safety injection pumps is required within two hours, requiring availability of the diesels. The difference between the long LOOP and the short LOOP is only in long term cooling after two hours, as the grid is recovered in the case of short LOOP.

  The frequency of short LOOP derived from EUR [Ref-1] is: LOOPS_AB: 6.0E-02/y. The frequency in shutdown states, derived using the durations of these reactor states, is:

  - LOOPS_CA = 3.9E-04/y

  - LOOPS_CB = 5.5E-04/y
  - LOOPS_D = 3.0E-04/y

- Long LOOP lasting less than 24 hours. The main grid is recovered within 24 hours.

  In the LOOP fault sequence model, if the plant operates for two hours and offsite power is not recovered within this two-hour period, the plant response model requires a stable state to be maintained for the 24 hour mission time. This is required for the plant to reach a final successful stable state.

  The frequency of long LOOP derived from EUR [Ref-1] is: LOOPL_AB = 1.0E-03/y. The frequency in shutdown states, derived using the duration of the reactor states, is:

  - LOOPL_CA = 6.5E-06/y
  - LOOPL_CB = 9.1E-06/y
  - LOOPL_D = 5.0E-06/y

Loss of Offsite Power in reactor state E is not considered. The reactor pool is full of water and, the water inventory above the core is sufficient to ensure the heat removal without any additional cooling systems:

- firstly by the heating of the water to saturation conditions;
- secondly by the boiling of the water.

There will be more than three days before the core uncovers, during which appropriate recovery actions can be taken.

4.5.3. Consequential LOOP

The PSA addresses the potential loss of main grid due to a sudden loss of the grid connection. A “consequential LOOP” is also postulated following a spurious reactor trip (RT), Turbine Trip (TT), loss of main feedwater (LOMFW) or loss of condenser (LOC) events. A conditional probability of a consequential LOOP of 1.0E-03/demand is assumed, derived from UK operational experience feedback [Ref-1]. It is assumed that one out of three consequential LOOP events leads to short LOOP and two out of three consequential LOOP events lead to long LOOP [Ref-2]. The conditional probabilities used in the event tree model are:

- Conditional Short LOOP: 1E-03 x 1/3 = 3.33E-04/d
- Conditional Long LOOP: 1E-03 x 2/3 = 6.67E-04/d

Following a loss of main grid the process of transferring to house load is automatically initiated. However, this potential backup is conservatively ignored in the PSA.

LOOP events lasting more than 24 hours are assumed to be possible due to external hazards. These are considered in Sub-chapter 15.2.

4.6. PRIMARY TRANSIENTS

These transients are defined by the following initiating events:

4.6.1. Spurious Reactor Trip (RT)

The frequency of Reactor Trip during power operation is assigned a value of {CCI} [a]. This frequency covers several types of initiating event due to human operating error, during testing, preventive maintenance etc, leading to a spurious reactor trip. The following events are included in this grouping:

- Spurious actuation of the pressuriser spray,
- Spurious withdrawal of one Control rod assembly (RCCA),
- Spurious safety injection.
- Spurious isolation of the RCV [CVCS] letdown line.

4.6.2. Boron dilution (BDIL)

In Pressurised Water Reactors, the excess reactivity of the fuel is compensated mainly by soluble boron (acid) dissolved in the primary coolant. The boron acts as a neutron absorber. Starting at a maximum level at the start of a new fuel cycle, the excess reactivity progressively decreases with the increase in core burn-up. The boron concentration in the primary circuit is accordingly reduced down to near zero at the end of the cycle. In addition, dissolved boron is also used to:

- compensate for the increase in reactivity in going from hot to cold conditions

and

- to ensure sufficient subcriticality during cold shutdown states.

Consequently, the possibility exists for generating a large positive reactivity transient by inadvertently introducing cold or unborated water into the core. Such a reactivity transient could lead to a power excursion with potentially severe consequences for the core and in principle, under extreme circumstances, for the environment.

The magnitude of the power excursion depends generally on the rate of the boron dilution and on the duration of the event. When considering boron dilution faults it is useful to distinguish between different modes and types of dilution. Two modes can be defined:

- Homogeneous boron dilution;
- Heterogeneous boron dilution.

These scenarios are presented in TR 04/138 [Ref-1].

The sources of boron dilution investigated are:

- o Chemical volume control system (RCV [CVCS])

- o Low head safety injection in RHR operation (LHSI/RHR)
- o Component cooling water system RRI [CCWS]
- o Maintenance procedures on RCP [RCS].

4.6.2.1. Heterogeneous Boron Dilution

The current PSA model considers that:

- During full power operation (state A), the initiating event frequency for formation of an unborated water plug is {CCI} [a], see TR 04/138 [Ref-1].
- In shutdown state Ca, the initiating event frequency for formation of an unborated water plug is {CCI} [a], see TR 04/138 [Ref-1].

The major initiating events investigated in the PSA are presented in Section 15.1.4 - Table 3.

A new safety case for heterogeneous boron dilution events has been developed in GDA, which is described in section 7 of PCSR Sub-chapter 16.4. The safety case re-evaluates the frequency of injection of a diluted boron slug into the primary loop pipework in at-power and shutdown states using conservative assumptions, and introduces additional protection measures to prevent an unborated slug in the loop pipework from entering the core on restart of the Main Coolant Pumps. The current PSA model has not been modified to take into account the revised safety case or plant modifications. This is because, taking account of the revised event frequencies and protection measures presented in section 7 of PCSR Sub-chapter 16.4, the CDF contribution due to heterogeneous boron dilution events is expected to remain similar to that currently calculated.

The revised initiating event frequencies and protection system modifications will be incorporated into the PSA during the site licensing phase.

4.6.2.2. Homogeneous Boron Dilution

Homogeneous boron dilution could be caused by malfunction of the RCV [CVCS]/REA [RBWMS].

Two potential sources of Homogeneous Boron Dilution are analysed in the PSA:

- Homogeneous Dilution due to the Reactor Boron and Water Make-up System (REA [RBWMS]) via the Chemical and Volume Control System (RCV [CVCS]) with a maximum dilution rate of 36 to 100 tonnes per hour. This corresponds to the maximum flow rate from the RCV [CVCS] charging pump(s). (The Demineralised Water System pumps have a greater flow rate than the RCV [CVCS] charging pumps so the maximum flow rate is limited by the RCV [CVCS] flow rate).

  This dilution is isolatable by operation of isolation valves on the volume control tank or by operation of the reactor boron and water make-up system limitation devices.

  From French operating experience [Ref-1] the frequency of such dilution events is:

{CCI removed}

{CCI removed}

a

- Homogeneous Dilution, due to leakage in a heat exchanger cooled by the component cooling water system. Such a leakage could occur when the RCP [RCS] water purification process is initiated during plant shutdown. Some of these dilution events will have negligible consequences due to their limited size. Only the case of tube rupture in the condenser or the degasification unit gas cooler is analysed. The assumed flow rate is 15 tonnes per hour [Ref-1].

  This dilution is isolatable by operation of isolation valves on the volume control tank.

  The frequency of such failures, inferred from observed heat exchanger tube leak frequencies, is as follows:

{CCI removed}

a

4.6.2.3. Boron dilution scenarios during shutdown states that are screened out

Dilution in shutdown state C and D

This scenario involves a leak on an LHSI pump heat exchanger that is not detected by the boron meter. When the RHR pump is in operation a dilution event can occur following a leak in the heat exchanger associated with the pump, but the flow rate is very low (< 2.5 m^3/hour).

The time to reach criticality following this failure is always greater than 24 hours, based on calculations using conservative assumptions for the initial boron concentration, the reactor coolant system water inventory and assuming a leak rate of 3 m^3/hour. Therefore this dilution scenario is not included in the PSA.

Dilution in shutdown state E

In plant state E, the RCP [RCS] is open and the water in the IRWST (around 1800 m^3) is transferred into the reactor cavity. The RCP [RCS] inventory is thus very high and the boron concentration is also high at approximately 2000 ppm. The volume of demineralised water needed to dilute the RCP [RCS] inventory homogeneously to produce criticality is estimated at approximately 200 m^3.

One possible cause of such a dilution event is loss of inventory from a system in the reactor building that contains unborated water due to a large leak. The water would arrive in the IRWST through vent holes located on its edges. The ruptured system could be a fire protection system, a "service" water system, a secondary water system, a chilled water system, or the RRI [CCWS]. The volume of unborated water required to dilute the IRWST water homogeneously to 90% of its required boron concentration is about 200 m^3. Such an inventory loss would be highly unlikely to occur without being detected, either from anomalous behaviour of the system itself, or via other means including human surveillance. The ratio between the volume of the IRWST and the volume of the systems containing unborated water is so large that defence against the risk of a significant dilution of the IRWST is considered adequate.

Another potential cause of dilution events is a "loss" of unborated water caused by operator action during a maintenance operation. As in the case discussed above, the large capacity of the reactor pool provides a high level of intrinsic protection against the risk of a significant dilution. Nevertheless, the use of unborated water during maintenance operations in the reactor building is controlled and limited as far as possible. The risk of dilution of the reactor pool when the pool walls are being cleaned with demineralised water has been specifically considered. Following draining of the reactor pool, the pool walls are sprayed manually using a mobile high pressure cleaning unit (Kärcher type). The amount of water used for the cleaning, and the capacity of the tank involved in the cleaning process, are far too small to induce a significant homogeneous boron dilution. It should be noted that the use of such mobile cleaning units is not limited to the pool walls but applies also to the cleaning of other items of equipment which are removed from the pool water (e.g. slot gates, lifting rigs). In all cases the amounts of water involved are too small to cause significant boron dilution.

A third possible cause of dilution of the reactor pool is dilution due to PTR [FPCS] operation. This is potentially linked to the IRWST, and more specifically to the purification unit of the RCV [CVCS]. As discussed above, it is judged that the large capacity of the reactor pool provides sufficient defence against the risk of significant dilution from such an event.

4.6.3. Loss of Residual Heat Removal in Shutdown States – LORHR

When the reactor is shut down the residual heat removal function is provided either by the steam generators in plant state B, or by the Residual Heat Removal System (RHRS) in shutdown states C, D and E. In the EPR design, the RHRS is part of the Low Head Safety Injection system (LHSI).

Note: The loss of the heat removal function in plant state B is covered by the initiating event: loss of Start-up and shutdown feed system in state B (LOSSS_B).

The LORHR event family covers the loss of the RHR mission in plant states C, D and E.

Without mitigation, the consequences of a LORHR initiating event are:

- An increase in primary temperature (and pressure in state Ca and Cb);
- RCP [RCS] water boiling and an RCP [RCS] water level decrease;
- Fuel uncovery leading to core damage.

The development of this type of transient depends on the initial primary water inventory. In plant state E, the reactor pool is filled with water to allow the discharge or reload of fuel assemblies. The time available to recover the RHR function before potential core uncovery is thus very long, as in the case of LOOP in shutdown state E discussed in sub-section 4.5.2 of this sub-chapter. Consequently the PSA does not include LORHR in state E.

Loss of RHR is assumed to require the simultaneous failure of all of the circuits of the LHSI/RHR trains which are in RHR operation. The failure is assumed to be due to the LHSI system (RIS [SIS]) itself and not due to failure of supporting systems such as power supplies or cooling systems. Failures in such support systems are considered separately in the analysis of the Loss of Cooling Chain (LOCC) and Loss of Offsite Power (LOOP) fault groups.

The following table shows the LHSI/RHR trains which are operating in each shutdown state and the corresponding IE frequencies for LORHR.

Initiating Event	Operating trains	Frequency [/ry]
LORHR_CA	Loss of 4 out of 4 operating trains	{CCI} [a]
LORHR_CB	Loss of 3 out of 3 operating trains	{CCI} [a]
LORHR_D	Loss of 3 out of 3 operating trains	{CCI} [a]

4.6.4. Uncontrolled Level Drop (ULD)

The initiating event “Uncontrolled Level Drop” is defined as a fault affecting the reactor coolant water level, when the level has been intentionally decreased for operational purposes to the 3/4-loop level. This could occur in plant state Cb at the end of the level reduction, and in state D where the water level is being maintained at mid-loop. 3/4-loop operation is implemented during shutdown for SG tube draining and N2 flushing. A ULD event can be caused by the following:

- In state Cb, by failure to close the letdown line of the CVCS when the mid-loop level has been reached after a level decrease. This failure would be caused by failure of the operator to manually close the isolation valve successfully when required.

- In state D, by spurious opening of the isolation valve.

The frequencies of these two initiating events are evaluated by fault tree analysis as follows:

- In plant state Cb the frequency of ULD is calculated as {CCI} [a]. This includes failure of the operator, failure of the valve {CCI removed} [a] and failure of the level sensors {CCI removed} [a]. Because the same level sensors are used in both the protection system for automatic closure of the draining route, and for safety injection, a dependency has been modelled in the PSA.

  2.4 drains per year are assumed for the calculation of the initiating event frequency.

- In state D the frequency of ULD is calculated as {CCI} [a]. This covers only the failures due to failure of the valve.

4.7. LOSS OF COOLING CHAIN (LOCC)

Loss of RRI [CCWS] or SEC [ESWS] is modelled as a Loss of Cooling Chain (LOCC) initiating event. These support system initiating events are important because of the impact they have on other systems and components. Their failure can result in a loss of cooling to the reactor coolant pumps, safeguards building room cooling chillers, RCV [CVCS] pumps, and RIS [SIS] pumps. Several different LOCC initiating events are modelled to capture different combinations of system failure modes, from the loss of a single train to loss of all four trains. The impact of the initiating events also depends on isolation if the initiating event involves a leak. Success or failure of isolation and its respective impact is incorporated into the development of the event tree and/or the fault tree models as appropriate.

Note that in the PSA model the initiating events and their consequences are modelled assuming Divisions 1 and 4 of the RRI [CCWS] are operating and Divisions 2 and 3 are on standby with their isolation valves to the common headers closed. In addition, RCV [CVCS] pump 1 cooled from RRI [CCWS] common header 1 (Divisions 1 and 2 RRI) is assumed to be operating and RCV [CVCS] pump 2 cooled from RRI common header 2 (Divisions 3 and 4 RRI [CCWS]) is assumed to be on standby. Preventive maintenance on train 2 of the cooling chain is considered in the assessment of the initiating event frequency.

Event frequencies are evaluated from fault tree analysis. 7 types of LOCC IE are studied:

A loss of one out of two common user headers (LOCC1, LOCC2, LOCC3, LOCC4) due to:

- An RRI [CCWS] leak from its tank which is not automatically made up;
- Mechanical failure;
- Preventive maintenance;
- I&C failure (failure of SPPA-T2000 I&C used for switchover of common user header feed to RRI [CCWS] standby train).

A loss of the two common user headers (suddenly or progressively) (LOCC5, LOCC6, LOCC7); this loss results from the loss of one header combined with the failure of the second header while the first is being repaired. The main causes of the loss of the two headers are presented in the following table, grouped according to the minimum number of available RRI/SEC [CCWS/ESWS].

The LOCC events are analysed for at-power operating states (A and B). A total loss of the cooling chain (LOCC7) is studied for shutdown states (Ca, Cb and D) when all LHSI/RHR trains are connected. Partial loss of cooling chain is not considered for shutdown states Ca, Cb and D as one LHSI/RHR train is sufficient for heat removal.

LOCC in state E is not analysed in the PSA for the same reason that the LORHR and LOOP are not considered i.e. the large water inventory present in the reactor pool (see sub-section 4.5.2 of this sub-chapter).

Failure of the automatic switchover of common user header feed to RRI [CCWS] standby train is considered in LOCC Initiating Events by introducing a dependency to the non-specific processing part of SPPA-T2000 I&C platform. Events identified as LOCC3B, LOCC5B, LOCC6B and LOCC7B represent the failure of the mechanical parts of RRI [CCWS] which in association with the failure of SPPA-T2000 switchover signal, induce the corresponding LOCCi (i=3, 5, 6 or 7) Initiating Event.

Initiating event	Causes	Frequency [/ry] in power states A&B	Frequency [/ry] in shutdown states CA, CB, D
LOCC1	Leak of one common user header out of two	{CCI}[a]	-
LOCC2	Leak of one operating RRI [CCWS] train out of two	{CCI}[a]	-
LOCC3 (including LOCC3B)	Unavailability of one common user header out of two due to failure of operating RRI/SEC [CCWS/ESWS] train and failure of switchover of the common user header feed	{CCI}[a]	-
LOCC4	Unavailability of one common user header out of two due to failure of the operating RRI/SEC [CCWS/ESWS] train and failure of the backup train (incl. preventive maintenance)	{CCI}[a]	-
LOCC5 (including LOCC5B)	Leaks from two common user headers Leak from one common user header & leak of the operating RRI [CCWS] train which supplies the other common user header Leak from one common user header & unavailability of the other common user header due to the failure of the operating RRI/SEC [CCWS/ESWS] train and of the switchover of the common user header feed	{CCI}[a]	-
LOCC6 (including LOCC6B)	Leak from one common user header & unavailability of the other common user header due to the failure of its two RRI/SEC [CCWS/ESWS] trains Leaks from the two operating RRI [CCWS] trains Leak from two operating RRI [CCWS] train & unavailability of the other common user header due to the failure of the operating RRI/SEC [CCWS/ESWS] train and of the switchover of the common user header feed Failure of the two operating RRI/SEC [CCWS/ESWS] trains and failure of the switchovers of the two common user header feeds	{CCI}[a]	-

Initiating event	Causes	Frequency [/ry] in power states A&B	Frequency [/ry] in shutdown states CA, CB, D
LOCC 7 (including LOCC7B [2])	Leak from the operating RRI [CCWS] train and unavailability of the other common user header due to the failure of the operating RRI/SEC [CCWS/ESWS] train and of the backup train. Failure of the two operating RRI/SEC [CCWS/ESWS] trains & failure of the switchover of the feed to one common user header & failure of the backup RRI [CCWS] train to feed the other common user header. Failure of the two RRI/SEC [CCWS/ESWS] operating trains and failure of the two RRI/SEC [CCWS/ESWS] backup trains (incl. preventive maintenance).	{CCI}^{a}	
	In shutdown states the failure of the four operating trains corresponds to the failure to run of the RRI [CCWS] pumps or the SEC [ESWS] pumps.		{CCI}^{a}

4.8. ANTICIPATED TRANSIENTS WITHOUT SCRAM (ATWS)

The ATWS fault group covers transients requiring a reactor trip but where a failure to drop all or some control rods occurs. ATWS initiating events are studied [Ref-1] for the following groups of transients:

- Total Loss of Main Feedwater initiating events:
  - Total loss of Main Feedwater pumps (LOMFW)

[2] A LOCC7B_AB Initiating event was developed in a separate Event Tree. The LOCC7B_AB Initiating Event conservatively considers the 4 RRI/SEC [CCWS/ESWS] trains to be unavailable, while in reality, in some cases (including a failure of switchover of common user header feed to RRI [CCWS] standby train due to I&C failure), one RRI/SEC [CCWS/ESWS] train would still be available for cooling the corresponding MHSI pump. The case with failure of switchover due to I&C failure is therefore specifically modelled in the Event Tree LOCC7B_AB.

  - Loss of condenser vacuum (LOC)
  - Loss of Extraction Circuit (CEX) pumps (grouped with LOC events)
- Loss of Secondary Load:
  - Turbine Trip with GCT [MSB] available (TT)
- Excess steam flow rate:
  - Excess steam demand by the turbine (grouped with SLB_SO)
  - Spurious opening of the GCT [MSB] (SLB_SO)
  - Spurious opening of the VDA [MSRT] (SLB_SO)
  - Spurious Safety Injection (grouped with RT)
- Loss of the main electrical power grid:
  - Loss of the main electrical power grid without taking credit of house load
  - Loss of the step-down transformer (LOOP)
- Reactor coolant pressure transients:
  - Spurious actuation of pressuriser spray (grouped with RT)
- Primary Breaks – LOCA:
  - 2A-LOCA (PBL-2A)
  - Large break [180 – 830 cm²] (PBL1)
  - Medium break [45 – 180 cm²] (PBM1 and PBM2)
  - Small break [2 – 45 cm²] (PBS)
- Steam Generator Tube Rupture:
  - SGTR 1 tube (SGTR1)
  - SGTR 2 tubes (SGTR2)

Section 15.1.4 - Table 2 summarises the ATWS initiating events considered in the PSA.

SECTION 15.1.4 - TABLE 1

Interfacing System LOCA events considered in Power States [Ref-1]

SYSTEM	TITLE	FREQUENCY [/ry]
RCV [CVCS]	2 HP cooler tubes rupture and RCP [RCS] flow to the RRI [CCWS]	{CCI}^{a}
	1 HP cooler tube rupture and RCP [RCS] flow to the RRI [CCWS]	{CCI}^{a}
	Spurious full opening of the reducing station	{CCI}^{a}
	Rupture of the charging line (DN 100 mm) between the control valve and the containment, and back flow from the charging line	{CCI}^{a}
	Leakage from the charging line outside the containment (DN 100 mm) downstream of control valve, and back flow from the charging line.	{CCI}^{a}
	Rupture of the charging line outside the containment (DN 100 mm) downstream of the control valve, and back flow from the seal injection line.	{CCI}^{a}
	Rupture upstream of the control valve on the charging line (DN 100 mm) up to the three way valve and on the seal injection line (DN 50 mm) up to the containment and back flow from the charging line	{CCI}^{a}
	Leakage upstream of the control valve on the charging line (DN 100 mm) up to the three way valve and on the seal injection line (DN 50 mm) up to the containment and back flow from the charging line	{CCI}^{a}
	Rupture upstream of the control valve on the charging line (DN 100 mm) up to the three way valve and on the seal injection line (DN 50 mm) up to the containment and back flow from the seal injection line	{CCI}^{a}
	Leakage upstream of the control valve on the charging line (DN 100 mm) up to the three way valve and on the seal injection line (DN 50 mm) up to the containment and back flow from the seal injection line	{CCI}^{a}
RIS [SIS]	Failure of the three isolation check-valves and consequent rupture of the MHSI line.	{CCI}^{a}
	Following actuation of MHSI, back flow from RCP [RCS] to MHSI line	{CCI}^{a}
	Failure of the three isolation check-valves and consequent rupture on LHSI line.	{CCI}^{a}
	Rupture of the LHSI line consequent upon actuation of MHSI	{CCI}^{a}

SYSTEM	TITLE	FREQUENCY [/ry]
	Back flow from the RCP [RCS] to the RHR line and consequent rupture downstream of RIS1615VP	{CCI}[a]
	Back flow from the RCP [RCS] to the RHR line and rupture of the pipe upstream of RIS1615VP	{CCI}[a]
	Back flow from the RCP [RCS] to the RHR line and leakage of the pipe upstream of RIS1615VP	{CCI}[a]
RBS [EBS]	Back flow from the RCP [RCS] and consequent rupture upstream RBS [EBS] pump	{CCI}[a]
	Back flow from the RCP [RCS] inducing a rupture of RBS [EBS] pipe outside containment (DN 50 mm) downstream of the pump and back flow from the RCP [RCS].	{CCI}[a]
	Leakage of RBS [EBS] pipe outside containment (DN 50 mm) downstream of the pump and back flow from the RCP [RCS].	{CCI}[a]
	RBS [EBS] start up and normal stop and rupture upstream of the RBS [EBS] pump	{CCI}[a]
	RBS [EBS] start up and normal stop and rupture downstream of the RBS [EBS] pump	{CCI}[a]
	RBS [EBS] start up and normal stop (including spurious actuation) and leakage downstream of the RBS [EBS] pump	{CCI}[a]
RRI [CCWS]	Rupture of 2 tubes of the thermal barrier, back flow from the RCP [RCS] and consequent rupture on the RRI [CCWS] side upstream thermal barrier.	{CCI}[a]
	Rupture of 1 tube of the thermal barrier, back flow from the RCP [RCS] and consequent rupture on the RRI side upstream of thermal barrier.	{CCI}[a]
	Rupture of 2 tubes of the thermal barrier, back flow from the RCP [RCS] and consequent rupture on the RRI side upstream of thermal barrier.	{CCI}[a]
	Rupture of 1 tube of the thermal barrier, back flow from the RCP [RCS] and consequent rupture on the RRI [CCWS] side upstream of thermal barrier.	{CCI}[a]
EVU [CHRS]	Actuation of EVU [CHRS] and rupture on the main pipework	{CCI}[a]
	Actuation of EVU [CHRS] and leakage the main pipe or external leakage from components	{CCI}[a]
TOTAL		{CCI}[a]

SECTION 15.1.4 - TABLE 2

ATWS initiating events addressed in the PSA

ATWS group in the PSA	Initiating events addressed	Freq. [/y]	[Ref-1] to [Ref-5]	Codification and Frequency [/y]
Loss of Main feedwater - LMF	LOMFW	{CCI}[a]	FA3	WS_LMF {CCI}[a]
	Loss of condenser vacuum	1.0E-01	EUR	
	Loss of Extraction Circuit (CEX) pumps	5.0E-02	EUR	
Loss of Secondary Load	Turbine Trip with GCT [MSB] available (TT)	{CCI}[a]	FA3	WS_TT {CCI}[a]
Excess steam flow	Excess steam demand by the turbine	{CCI}[a]	FA3	WS_ISF {CCI}[a]
	Spurious opening of the GCT [MSB]			
	Spurious opening of a VDA [MSRT] or a VVP [MSSV]			
	Spurious Safety Injection (grouped with RT)	{CCI}[a]	FA3	WS_SSI {CCI}[a]
Loss of the main electrical power grid	Loss of the main electrical power grid with house load failure	{CCI}[a]	FA3	WS_LOP {CCI}[a]
	Loss of the step-down transformer			
Reactor coolant pressure transients	Spurious pressurised spray (grouped with RT)	{CCI}[a]	FA3	WS_PT1 {CCI}[a]
Primary Breaks	2A-LOCA	{CCI}[a]	Expert Judgment	WS_PB {CCI}[a]
	Large break [180 – 830 cm²]	1.3E-06	NUREG	
	Medium break [45 – 180 cm²]	1.6E-05	NUREG	
	Small break [20 – 45 cm²]	6.04E-04	NUREG	
	Small break [2 – 20 cm²]	5.77E-04	NUREG	
	PZR leak	{CCI}[a]	AREVA	

ATWS group in the PSA	**Initiating events addressed**	**Freq. [/y]**	**[Ref-1] to [Ref-5]**	**Codification and Frequency [/y]**
Steam Generator Tube Rupture	SGTR 1 tube	{CCI}[a]	FA3	WS_SGTR {CCI}[a]
	SGTR 2 tubes	{CCI}[a]	FA3	

SECTION 15.1.4 - TABLE 3

Major Heterogeneous Boron dilution scenarios addressed in the PSA [Ref-1]

Boron Dilution from	Description	Occurrence Frequency [/ry]	
		States A&B	States C
RCV [CVCS]	Operator error in adjustment of boron concentration set point in REA [RBWMS]	{CCI}[a]	-
	Malfunction of the REA [RBWMS] control system.	{CCI}[a]	{CCI}[a]
	Incorrect boron concentration in the REA [RBWMS] tank.	{CCI}[a]	{CCI}[a]
	RCV [CVCS] HP-Cooler tube rupture	-	{CCI}[a]
	Non-compliance with procedures associated with commissioning of a demineraliser	{CCI}[a]	{CCI}[a]
	Residual low boron concentration water in the RCV [CVCS] system after maintenance	-	{CCI}[a]
	Tube rupture (RRI [CCWS] leak) in the condenser, gas cooler or the TEG [GWPS] gasification unit	{CCI}[a]	{CCI}[a]
	LOOP during normal dilution operations	{CCI}[a]	-
RIS/RRA [SIS/RHR]	Failure of RRA pump	-	{CCI}[a]
	Residual low boron concentration water in the RCV [CVCS] system after maintenance	-	{CCI}[a]
	Residual unborated water in the accumulators after maintenance	-	{CCI}[a]
RRI [CCWS]	Rupture of thermal barrier	-	{CCI}[a]
Environment (opening of RCP [RCS])	Residual low boron concentration water in the RCV [CVCS] system after maintenance	-	{CCI}[a]

SECTION 15.1.4 - TABLE 4

Summary of the Initiating Events studied in the PSA

INITIATING EVENT	Reactor state	CODIFICATION	FREQUENCY [/y]	REFERENCE
PRIMARY BREAKS				
2A-LOCA	A&B	PBL-2A_AB	{CCI}[a]	Expert Judgment based on HSE SAPs [Ref-1] and NUREG-1829 [Ref-2]
Large primary break [180 cm² - 830 cm²]	A&B	PBL1_AB	1.3E-06	NUREG/CR-6928 [Ref-3]
Medium/Large primary break [100 – 180 cm²]	A&B	PBM1_AB	8.0E-06	NUREG-1829 [Ref-2]
Medium/Small primary break [45 – 100 cm²]	A&B	PBM2_AB	8.0E-06	NUREG-1829 [Ref-2]
Pressuriser leak (stuck open PSRV)	A&B	PBPZR_AB	{CCI}[a]	NEPSF DC 109 [Ref-4]
Pressuriser leak (stuck open PSRV)	CA	PBPZR_CA	{CCI}[a]	NEPSF DC 109 [Ref-4]
Small primary breaks [2 – 45 cm²]	A&B	PBS_AB	1.18E-03	NUREG-1829 [Ref-2] and NUREG/CR-6928 [Ref-3]
Small primary breaks [2 – 20 cm²]	CA	PBS_CA	3.9E-06	NUREG/CR-6928 [Ref-3]
Small primary breaks [2 – 20 cm²]	CB	PBS_CB	5.5E-06	NUREG/CR-6928 [Ref-3]
Small primary breaks [2 – 20 cm²]	D	PBS_D	3.0E-06	NUREG/CR-6928 [Ref-3]

INITIATING EVENT	Reactor state	CODIFICATION	FREQUENCY [/y]	REFERENCE
Small primary breaks [2 – 20 cm²]	E	PBS_E	8.3E-06	NUREG/CR-6928 [Ref-3]
Reactor Pressure Vessel Failure	All	RPV	{CCI}[a]	Expert Judgment
Interfacing system LOCA – V-LOCA during power operation	A&B	PBV_AB	{CCI}[a]	EPSE DC 833 [Ref-5]
Interfacing system LOCA – V-LOCA Small external break (5 – 20 cm²) on the ISBP/RRA	CA	PBV1_CA	{CCI}[a]	German Exp. [Ref-6]
	CB	PBV1_CB	{CCI}[a]	German Exp. [Ref-6]
	D	PBV1_D	{CCI}[a]	German Exp. [Ref-6]
	E	PBV1_E	{CCI}[a]	German Exp. [Ref-6]
Interfacing system LOCA – V-LOCA Significant external break (20 cm² and breaks of a diameter equal to DN250 (size of LHSI/RHR lines) on the ISBP/RRA	CA	PBV2_CA	{CCI}[a]	German Exp. [Ref-6]
	CB	PBV2_CB	{CCI}[a]	German Exp. [Ref-6]
	D	PBV2_D	{CCI}[a]	German Exp. [Ref-6]
	E	PBV2_E	{CCI}[a]	German Exp. [Ref-6]
Rupture of two tubes on the SIS/RHR heat exchanger in state C.	C	PBV3_C	{CCI}[a]	Fault Tree analysis
STEAM GENERATOR TUBE RUPTURE – SGTR				
1 Steam Generator Tube Rupture	A&B	SGTR1_AB	{CCI}[a]	FA3 [Ref-7]

INITIATING EVENT	Reactor state	CODIFICATION	FREQUENCY [/y]	REFERENCE
2 Steam Generator Tube Rupture	A&B	SGTR2_AB	{CCI}[a]	FA3 [Ref-7]
PRIMARY TRANSIENTS				
Spurious Reactor Trip Including: Spurious actuation of pressuriser spray. Spurious withdrawal of 1 Control rod assembly. Spurious safety injection. Spurious isolation of CVCS letdown line.	A	RT_A	{CCI}[a]	Expert judgment based on operating experience
Heterogeneous boron dilution	A	DIL HE_A	{CCI}[a]	TR 04/138 [Ref-8]
Heterogeneous boron dilution	CA	DIL HE_CA	{CCI}[a]	TR 04/138 [Ref-8]
Homogeneous boron dilution	A	DIL HO_A	{CCI}[a]	FA3 [Ref-7]
Homogeneous boron dilution, CCWS break, 15 te/h	B	DIL HO15_B	{CCI}[a]	FA3 [Ref-7]
Homogeneous boron dilution, CCWS break, 15 te/h	CA	DIL HO15_CA	{CCI}[a]	FA3 [Ref-7]
Homogeneous boron dilution, CCWS break, 15 te/h	CB	DIL HO15_CB	{CCI}[a]	FA3 [Ref-7]
Homogeneous boron dilution, RBWMS dilution, 100 te/h	B	DIL HO100_B	{CCI}[a]	FA3 [Ref-7]

INITIATING EVENT	Reactor state	CODIFICATION	FREQUENCY [/y]	REFERENCE
Homogeneous boron dilution, RBWMS dilution, 72 te/h	CA	DIL HO72_D	{CCI}[a]	FA3 [Ref-7]
Homogeneous boron dilution, RBWMS dilution, 36 te/h	CB	DIL HO36_CB	{CCI}[a]	FA3 [Ref-7]
Homogeneous boron dilution, RBWMS dilution, 36 te/h	D	DIL HO36_D	{CCI}[a]	FA3 [Ref-7]
Loss of 4/4 operating LHSI/RHR trains	CA	LORHR_CA	{CCI}[a]	Fault tree analysis
Loss of 3/3 operating LHSI/RHR trains	CB	LORHR_CB	{CCI}[a]	Fault tree analysis
Loss of 3/3 operating LHSI/RHR trains	D	LORHR_D	{CCI}[a]	Fault tree analysis
Uncontrolled Level Drop	CB	ULD_CB	{CCI}[a]	Fault tree analysis and FA3 [Ref-7]
Uncontrolled Level Drop	D	ULD_D	{CCI}[a]	Fault tree analysis
LOSS OF COOLING CHAIN – LOCC				
Leak of one common user header out of 2	A&B	LOCC1_AB	{CCI}[a]	Fault tree analysis
Leak of one operating RRI [CCWS] train out of 2	A&B	LOCC2_AB	{CCI}[a]	Fault tree analysis
Unavailability of 1/2 common user header due to failure of operating RRI/SEC [CCWS/ESWS] train and failure of switchover of feed to the common user header	A&B	LOCC3_AB	{CCI}[a]	Fault tree analysis
Failure of operating CCWS train and failure of the backup CCWS train	A&B	LOCC4_AB	{CCI}[a]	Fault tree analysis

INITIATING EVENT	Reactor state	CODIFICATION	FREQUENCY [/y]	REFERENCE
Failure of 2 common headers, 3 RRI [CCWS] trains available	A&B	LOCC5_AB	{CCI}[a]	Fault tree analysis
Failure of 2/2 common headers, RRI [CCWS] trains available.	A&B	LOCC6_AB	{CCI}[a]	Fault tree analysis
Total loss of cooling chain (TLOCC)	A&B	LOCC 7_AB	{CCI}[a]	Fault tree analysis
	CA	LOCC 7_CA	{CCI}[a]	Fault tree analysis
	CB	LOCC 7_CB	{CCI}[a]	Fault tree analysis
	D	LOCC 7_D	{CCI}[a]	Fault tree analysis
Large Secondary line breaks inside containment	A&B	SLB_LI_AB	1.3E-06	NUREG/CR-6928 [Ref-3]
Large steam line breaks downstream of Main Steam Isolation Valves	A&B	SLB_LO_AB	{CCI}[a]	FA3 [Ref-7]
Small steam line break upstream Main Steam Isolation Valves Including: Small feedwater line breaks inside containment. Small feedwater line breaks inside containment, located between the last feedwater line check valve and the SG. Spurious opening of a Main Steam Relief Isolation Valve.	A&B	SLB_SO_AB	{CCI}[a]	FA3 [Ref-7]

INITIATING EVENT	Reactor state	CODIFICATION	FREQUENCY [/y]	REFERENCE
Main Steam Safety Valves (VVP [MSSS]) stuck-open.				
INDUCED STEAM GENERATOR TUBE RUPTURE				
SGTR induced by Large secondary side breaks inside containment	A&B	SLB_LI_SGTR_AB	{CCI}[a]	NUREG/CR-6928 [Ref-3]
SGTR induced by Large steam line breaks downstream Main Steam Isolation Valves	A&B	SLB_LO_SGTR _AB	{CCI}[a]	FA3 [Ref-7]
SGTR induced by Small steam line break upstream Main Steam Isolation Valves	A&B	SLB_SO_SGTR _AB	{CCI}[a]	FA3 [Ref-7]
SECONDARY SYSTEM TRANSIENTS				
Total Loss of Main SG Feedwater	A	LOMFW_A	{CCI}[a]	French operating experience
Total Loss of Start-up and Shutdown System	B	LOSSS_B	{CCI}[a]	FT analysis
Spurious Turbine Trip	A	TT_A	{CCI}[a]	FA3 [Ref-7]
Loss of condenser Including: Loss of condenser vacuum Loss of Circulating pumps	A&B	LOC_AB	1.5E-01	EUR Vol.2 Ch 17 [Ref-9]

INITIATING EVENT	Reactor state	CODIFICATION	FREQUENCY [/y]	REFERENCE
LOSS OF OFFSITE POWER – LOOP				
Short LOOP < 2 hours	A&B	LOOPS_AB	6E-02/y	EUR Vol.2 Ch 17 [Ref-9]
	CA	LOOPS_CA	3.9E-04/y	EUR Vol.2 Ch 17 [Ref-9]
	CB	LOOPS_CB	5.5E-04/y	EUR Vol.2 Ch 17 [Ref-9]
	D	LOOPS_D	3.0E-04/y	EUR Vol.2 Ch 17 [Ref-9]
Long LOOP < 24 hours	A&B	LOOPL_AB	1.0E-03/y	EUR Vol.2 Ch 17 [Ref-9]
	CA	LOOPL_CA	6.5E-06/y	EUR Vol.2 Ch 17 [Ref-9]
	CB	LOOPL _CB	9.1E-06/y	EUR Vol.2 Ch 17 [Ref-9]
	D	LOOPL_D	5.0E-06/y	EUR Vol.2 Ch 17 [Ref-9]
Induced LOOP (short)	A	LOOPS_AB	3.33E-04/d (conditional probability)	Expert Judgment (based on National Grid Report [Ref-10] and NUREG/CR-6890 [Ref-11])
Induced LOOP (long)	A	LOOPL_AB	6.67E-04/d (conditional probability)	
ANTICIPATED TRANSIENTS WITHOUT SCRAM – ATWS				
ATWS – Loss of Main Feedwater	A	WS_LMF	{CCI}[a]	Section 15.1.4 - Table 2

INITIATING EVENT	Reactor state	CODIFICATION	FREQUENCY [/y]	REFERENCE
ATWS – Turbine Trip	A	WS_TT	{CCI}[a]	Section 15.1.4 - Table 2
ATWS – Excess Steam Flow	A	WS_ISF	{CCI}[a]	Section 15.1.4 - Table 2
ATWS – Spurious Safety Injection	A	WS_SSI	{CCI}[a]	Section 15.1.4 - Table 2
ATWS – Loss of Main Power	A	WS_LOP	{CCI}[a]	Section 15.1.4 - Table 2
ATWS – Primary Transient / Spurious Pressuriser Spray	A	WS_PT1	{CCI}[a]	Section 15.1.4 - Table 2
ATWS – Primary Break	A	WS_PB	{CCI}[a]	Section 15.1.4 - Table 2
ATWS – Steam Generator Tube Rupture	A	WS_SGTR	{CCI}[a]	Section 15.1.4 - Table 2

5. ACCIDENT SEQUENCE ANALYSIS

5.1. PRIMARY BREAKS - LOCA

5.1.1. Group Description

The Loss of Coolant Accident (LOCA) group deals with initiating events corresponding to breaks in the Reactor Primary Coolant System (RCP [RCS]) where the Chemical and Volume Control System (RCV [CVCS]) is not capable of maintaining the water inventory.

The consequences of a break in the RCP [RCS] depend on the reactor state. The whole spectrum of LOCAs is analysed for at-power states A and B. Only Small Primary Breaks are analysed for shutdown states Ca, Cb, D and E.

During at-power states, a LOCA results in a depressurisation of the Reactor Coolant System, a decrease of pressuriser (PZR) level and an increase in the pressure in the containment. The mitigation systems halt power production by tripping the reactor and compensate for the break flow rate via the Safety Injection System (RIS [SIS]). The secondary side cools the primary system and lowers the RCP [RCS] pressure. Cooldown is performed by all SGs via steam dump to the condenser or to the atmosphere. The respective relief valve setpoints are decreased to a value low enough to allow the required safety injection

In shutdown states, a Small Primary Break leads to an RCP [RCS] pressure and level decrease that can affect the operability of the RIS-RA [LHSI/RHR] trains. The mitigation systems compensate for the break flow rate using the RIS [SIS] in injection mode.

The following initiating events are considered in the LOCA group:

- Small Primary Break in at-power states A and B [2-45 cm²] and in shutdown states Ca, Cb, D and E [2-20 cm²] (PBS-_AB, PBS-_CA, PBS-_CB, PBS-_D, PBS-_E).

- Pressuriser Leak (equivalent to a small LOCA) in at-power states A and B and in shutdown state Ca (PBSPZR-_AB, PBSPZR-_CA)

- Medium Primary Break [45-180 cm²] in at-power states A and B (PBM1-_AB, PBM2-_AB).

- Large Primary Break [180-830 cm²] in at-power states A and B (PBL1-_AB).

- 2A – Break [>830 cm²] in at-power states A and B (PBL-2A_AB)

- Reactor Pressure Vessel Failure (RPV_F)

The definition and frequencies of the initiating events are given in section 4 of this sub-chapter.

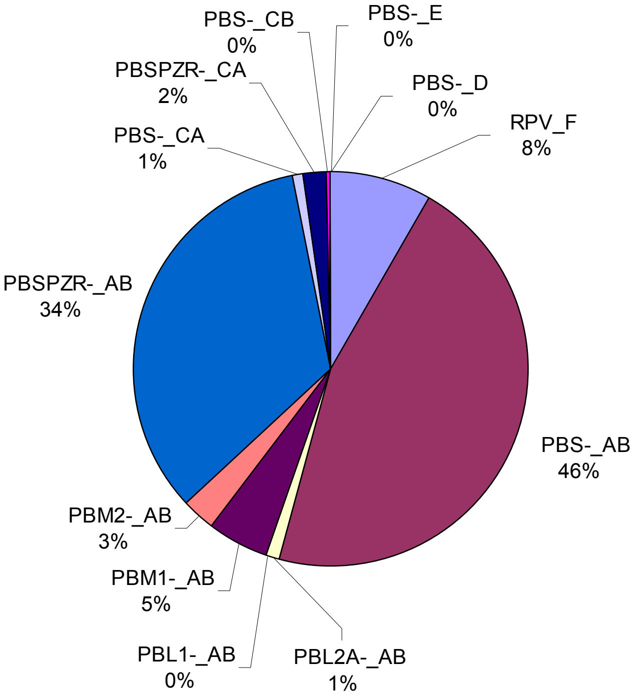
5.1.2. Results

The contribution of the Primary Break – LOCA group to the **Internal Event Core Damage Frequency is 1.18E-07/r.y**, which represents **22.2% of the Internal Event CDF**.

The CDF for each LOCA initiating event within the group is shown in the following table:

Initiating Event	IE frequency (/y)	CDF (/r.y)
RPV_F	{CCI}[a]	{CCI}[a]
PBL2A-_AB	{CCI}[a]	1.28E-09
PBL1-_AB	1.30E-06	5.85E-11
PBM1-_AB	8.00E-06	6.02E-09
PBM2-_AB	8.00E-06	3.18E-09
PBS-_AB	1.18E-03	5.40E-08
PBSPZR-_AB	{CCI}[a]	4.00E-08
PBS-_CA	3.90E-06	9.09E-10
PBSPZR-_CA	{CCI}[a]	2.53E-09
PBS-_CB	5.50E-06	3.57E-11
PBS-_D	3.00E-06	3.64E-11
PBS-_E	8.30E-06	1.17E-10
total		1.18E-07

The relative contribution of each LOCA initiating event within the group is given below:



5.1.3. Dominant Accident Sequence Analysis

The following table lists the dominant accident sequences in the Primary Break – LOCA group. Each accident sequence corresponds to one or a group of Minimal Cutsets (MCS). The main accident sequences considered in the table below account for 98% of the overall group risk.

Initiating event	***Brief description of the accident sequence***	***Frequency (per reactor per year)***
PBS-_AB or PBSPZR-_AB	The MHSI injection is unavailable due to Common Cause Failures (CCF) of the MHSI pumps or check valves **and** the operator fails to initiate Fast Cooldown to enable LHSI injection.	7.3E-08
PBS-_AB or PBSPZR-_AB	Partial Cooldown cannot be initiated because of secondary side failure (either mechanical failures including VDA [MSRT] trains, ASG [EFWS], GCT [MSB], AAD [SSS] or I&C followed by an operator failure) **so that** MHSI and LHSI pumps cannot inject into RCP [RCS] **and finally** the operator fails to initiate Feed and Bleed in 30 minutes.	1.9E-08
RPV_F	The failure of the reactor pressure vessel leads directly to unacceptable consequences. No recovery is considered in the level 1 PSA.	1.0E-08
PBM1-_AB	All MHSI trains are inoperable due to CCF or multiple single failures on pumps or check valves (i.e. 3 out of 3 MHSI trains; 1 train is lost due to the initiating event).	5.8E-09
PBS-_CA or PBSPZR-_CA	MHSI pumps fail to start and the 4 LHSI pumps in RHR mode fail to trip due to the same I&C failure **consequently** the MHSI and LHSI pumps cannot inject into the RCP [RCS].	3.4E-09
PBM2-_AB	All MHSI trains are inoperable due to CCF or multiple single failures on pumps or check valves (i.e. 1 out of 3 MHSI trains as 1 train is lost due to the initiating event) **and** the operator fails to initiate Fast Cooldown in 15 minutes.	3.1E-09
PBL-2A_AB	2 out of 3 MHSI trains (1 train is lost due to the initiating event) are inoperable due to CCF or multiple single failures on pumps or check valves.	1.1E-09

The dominant sequences show the importance of primary system breaks in at-power states. In these states, Medium-Head Safety Injection and partial or fast secondary cooldown are essential for the mitigation of the accident. The MHSI is required to compensate for the break flow rate when the pressure in the Reactor Coolant System has been reduced sufficiently by partial cooldown or by the break itself. If the MHSI trains are unavailable, a fast secondary cooldown has to be actuated by the operator to decrease the RCP [RCS] pressure sufficiently to allow LHSI injection into the cold legs. The time window available for the manual actuation of fast secondary cooldown depends on the break size and is insufficient for 100-180 cm² breaks (PBM1-_AB).

The dominant sequences show the limited contribution of failed partial cooldown sequences to the overall LOCA group risk. The diverse and redundant systems available for partial cooldown on the Steam Generator water side (AAD [SSS] and ASG [EFWS]) and steam side (VDA [MSRT] and GCT [MSB]) as well as the diverse I&C signals to actuate partial cooldown makes the partial cooldown highly reliable, which is essential for LOCA mitigation.

For shutdown states, the dominant cause of core damage is failure of the automatic makeup with MHSI and the failure to switchover the Low-Head Safety Injection from Residual Heat Removal mode to injection mode due to the same I&C failure (frequency: 3.4E-09/r.y)

5.1.4. Initiating Events Analysis

5.1.4.1. Small Primary Break – PBS

5.1.4.1.1. Event Description

At-power states

The initiating event "Small Primary Break" corresponds to the spectrum 2 cm^2 < LOCA ≤ 45 cm^2 and includes PZR leaks (PBS-_AB and PBSPZR-_AB).

A reactor trip occurs on low PZR pressure. The RT signal automatically trips the turbine and closes the Main Feedwater Full Load lines.

As the secondary side pressure increases, the Main Steam Bypass (GCT [MSB]) valves open initiating steam dump to the condenser. In the event of unavailability of steam dump to condenser, the Main Steam Relief Trains (VDA [MSRT]) open initiating steam dump to atmosphere.

The Steam Generators (SGs) are fed by the Main Feedwater System (ARE [MFWS]) through the Low Load control lines. In the event of unavailability of the ARE [MFWS], the start-up and shutdown (AAD [SSS]) pump starts and feeds the SG through the Low Load control lines. In the event of unavailability of the AAD [SSS], the ASG [EFWS] is actuated on low SG level.

A Safety Injection (SI) signal is actuated on very low PZR pressure (MIN3) or on very low hot leg pressure (MIN3). The SI signal automatically starts the MHSI and LHSI pumps, and initiates a partial cooldown of the secondary system. In the event of the failure of the I&C, the partial cooldown signal could be actuated by the operator. The partial cooldown cools the primary system and lowers the RCP [RCS] pressure.

During the partial cooldown, the RCP [RCS] pressure decreases sufficiently to allow MHSI injection into the cold legs. Partial cooldown is performed using all SGs via steam dump to the condenser or to the atmosphere. This is automatically controlled by decreasing the respective relief valve setpoints to achieve a constant cooling rate, until a fixed pressure value is reached. The final pressure is low enough to allow the required MHSI injection. If the MHSI trains are unavailable, a fast secondary cooldown is manually actuated to decrease the RCP [RCS] pressure sufficiently to allow the RIS [SIS] accumulators and the LHSI to inject into the cold legs. The operator can initiate Feed and Bleed in the event of failure of the secondary cooling and/or depressurisation to remove the heat and perform makeup.

Following partial cooldown the RCP [RCS] pressure remains constant, at least at the same level as the secondary side, until the break energy discharge rate is sufficient to remove the decay heat.

As long as the MHSI flow rate is insufficient to compensate for the break flow rate, the RCP [RCS] inventory continues to decrease. During this phase the break flow is sub-cooled and eventually reaches saturation conditions.

The break flow rate decreases as the void fraction in the cold legs increases. Eventually, the break flow changes to single steam phase. The RCP [RCS] inventory depletion stops when sufficient MHSI or LHSI flow is available to compensate for the break flow rate.

Shutdown states

Small Primary Breaks potentially affect the RHR safety function in all shutdown states. The consequences of the Small Primary Breaks depend on the reactor state.

For state Ca, a Small Primary break leads to a decrease in RCP level and pressure that threatens the operability of the RIS-RA [LHSI/RHR]. The situation requires makeup by the MHSI, actuated following a low delta-Psat signal, or the manual switchover of Low-Head safety injection from RHR to injection mode. If primary side RHR fails, due to loss of or automatic shutdown of the LHSI trains, RHR is performed by the steam generators. If secondary RHR fails, the operator initiates Feed and Bleed and cooling of the In-containment Refuelling Water Storage Tank (IRWST) using one RIS-RA [LHSI/RHR] train or the Containment Heat Removal system (EVU [CHRS]).

In state Cb, the break leads to an RCP [RCS] level decrease that threatens the operability of the RIS-RA [LHSI/RHR] trains. The situation requires makeup by either the MHSI trains, actuated following a low RCP [RCS] level signal, or manual switchover of the Low-Head safety injection from RHR to injection mode. Primary RHR is performed by cooling the IRWST with one RIS-RA [LHSI/RHR] train or one EVU [CHRS] train.

For state D, the situation requires makeup by either the MHSI trains actuated following a low RCP [RCS] level signal, or manual switchover of Low-Head safety injection from RHR to injection mode. The RCP [RCS] level decrease challenges the continued operability of the RIS-RA [LHSI/RHR] trains. Primary RHR is performed by cooling the IRWST with one RIS-RA [LHSI/RHR] train or one EVU [CHRS] train.

For state E, the response is as for state D.

5.1.4.1.2. Functional Safety Requirements

At-power states

This section identifies the safety functions that are challenged by Small Primary Breaks (2 - 45 cm^2) or PZR Leaks in at-power states:

- **Reactivity Control**: Reactivity control during the transient is provided by rod drop following the reactor trip signal.

  The consequences of the failure of rod drop are not considered in this section. They are considered in section 5.10 of this sub-chapter on Anticipated Transient Without Scram.

- Removal of core decay heat and stored heat. This safety function is divided into:

  - **Residual Heat Removal**: Residual heat removal is initially provided by the secondary side. It is achieved by feeding the steam generators with water and removing the steam produced. The following alternatives are available:

- for feeding the SGs, the Startup and Shutdown System (AAD [SSS]). In the event of failure of this system, the Emergency Feedwater System (ASG [EFWS]) starts automatically following a low low SG level signal. The PSA conservatively does not consider the Main Feedwater System (ARE [MFWS]).

- for removing steam from the SGs, the Main Steam Bypass (GCT [MSB]) for steam dump to condenser, the Main Steam Relief Valves (VDA [MSRT]) or the Main Steam Safety Valves for steam dump to atmosphere are available.

Note: The secondary side contributes to the RCP [RCS] inventory function by depressurising the primary side by partial or fast secondary cooldown.

The PSA considers Feed and Bleed in the event of partial cooldown failure.

o **Long term cooling**: The cooling of the IRWST is performed using the LHSI. In the event of unavailability of cooling with one LHSI train, cooling is provided by the Containment Heat Removal System (CHRS [EVU]).

- **Reactor Coolant System integrity**: the initiating event breaches the RCP [RCS].

- **Reactor Coolant System inventory control**: RCP [RCS] inventory control is provided by the Medium and Low-Head Safety Injection systems, including the RIS [SIS] accumulators.

  Prior to safety injection occurring, the pressure must be reduced in the RCP [RCS] via the secondary side by one of the following means:

  o Opening of the VDA [MSRT] by protection system signal or manual action or opening of the GCT [MSB] by safety automation signal for the partial cooldown if the MHSI is available (automatic actuation).

  o Opening of the VDA [MSRT] for the fast secondary cooldown if the MHSI is unavailable (manual actuation).

Shutdown states

This section identifies the safety functions that are challenged by Small Primary Breaks, states Ca to E, or a PZR Leak, state Ca only, in shutdown states:

Note: the Low Head Safety Injection pumps are the residual heat removal pumps.

- **Reactivity Control:** Reactivity control is not challenged by the transient.

- Removal of core decay heat and stored heat. This safety function is divided into:

  o **Residual Heat Removal**: For state Ca, after the automatic trip of the LHSI pump, residual heat removal is provided by opening the VDA [MSRT] valves at their cold shutdown setpoints. The valves discharge steam produced in the steam generators being fed by ASG [EFWS]. The PSA considers Feed and Bleed cooling in the event of failure of heat removal via the secondary side.

For states Cb to E, with automatic makeup via the MHSI, the RCP [RCS] level does not reach the LHSI pump trip level. Residual heat removal continues via the Residual Heat Removal (RIS-RA [RHR]) trains already in operation. The RHR train(s) in standby could also be put in service from the control room by the operator if required.

- o **Long term cooling**: Cooling of the IRWST is performed via the LHSI. In the event of unavailability of cooling by at least one LHSI train, cooling is carried out by the Containment Heat Removal System (CHRS [EVU]) (1 train).

- **Reactor Coolant System integrity**: the initiating event breaches the RCP [RCS].

- **Reactor Coolant System inventory control**: The automatic MHSI start-up on low delta-Psat for state Ca, or on low RCP level for states Cb to E, the RCP [RCS] rapidly restores the water inventory.

  In the event of failure of the MHSI, the LHSI in standby is manually started by the operator to provide makeup (states Ca to E).

5.1.4.1.3. Detailed Results

At-power states

A “Small Primary Break (2-45 cm^2) / PZR Leak” in an at-power state represents **17.7% of the Internal Event CDF, with a frequency of 9.40E-08/r.y.**

The following table lists the dominant accident sequences. Each accident sequence corresponds to one or a group of MCSs. The main accident sequences considered in the table below represent 98% of the initiating event risk.

Initiating event	***Brief description of the accident sequence***	***Frequency (per reactor per year)***
PBS-_AB and PBSPZR-_AB	MHSI injection fails due to a CCF on the MHSI pumps or check valves **and finally** the operator fails to initiate the fast secondary cooldown required to allow the LHSI injection.	7.3E-08
PBS-_AB and PBSPZR-_AB	Partial Cooldown cannot be initiated because of secondary side failure (either mechanical failures including VDA [MSRT] trains, ASG [EFWS], GCT [MSB], AAD [SSS] or I&C followed by an operator failure) **consequently** the MHSI and LHSI pumps cannot inject into the RCP [RCS] **and finally** the operator fails to initiate Feed and Bleed in 30 minutes.	1.9E-08

The following systems are important in the protection against Small Primary Breaks (2-45 cm^2) / PZR Leaks in at power states:

- **MHSI pumps and its cooling chain**. These systems are required to mitigate the LOCA: they compensate for the break flow and control the RCP [RCS] inventory. The MHSI pumps are essential in the event of Feed and Bleed.

- **Main Steam Relief Valves (VDA) [MSRV] or Main Steam Bypass (GCT [MSB])**. These systems are required to perform the partial or fast secondary cooldown and provide adequate steam release.

The following I&C signal or system is important in providing protection against Small Primary Breaks (2 - 45 cm^2) / PZR Leaks during power states:

- **"SG pressure > MAX1"**. Failure of this signal prevents control of partial cooldown. The PSA conservatively does not consider operator backup following this I&C failure. However the partial cooldown can also be started following the diverse signal **"hot leg pressure < MIN3"** and controlled by the GCT [MSB] controls (considered in the GCT [MSB] failure rate).

- **"SPPA-T2000"**. Failure of this platform makes the manual initiation of fast secondary cooldown impossible..

The following operator actions are important to protection against Small Primary Breaks (2 - 45 cm^2) / PZR Leaks during power states:

- The **operator initiates Fast Secondary Cooldown**. This action is required following failure of MHSI to decrease the RCP [RCS] pressure sufficiently to allow LHSI injection into cold legs.

- The **operator initiates Feed and Bleed**. Following failure of the secondary cooling and/or depressurisation, the operator must initiate Feed and Bleed to remove the heat and perform makeup.

Shutdown states

A "Small Primary Break or PZR Leak" occurring in a shutdown state represents **0.7% of the Internal Event CDF, with a frequency of 3.63E-09/r.y.**

The table below lists the dominant accident sequence which represents 90% of the initiating event risk.

Initiating event	***Brief description of the accident sequence***	***Frequency (per reactor per year)***
PBS-_CA or PBSPZR-_CA	MHSI pumps fail to start and the 4 LHSI pumps in RHR mode fail to trip due to the same I&C failure **consequently** the MHSI and LHSI pumps cannot inject into the RCP [RCS].	3.3E-09

State Ca is an important contributor to the overall risk in the event of Small Primary Breaks or PZR Leaks in shutdown states.

The following I&C signal is important in the protection against Small Primary Breaks or PZR Leaks in shutdown states:

- **"Low delta-Psat"**. Failure of this signal prevents the MHSI pumps from starting and RHR pumps in operation from being realigned to inject into cold legs in LHSI mode. Consequently MHSI and LHSI pumps are unavailable to compensate for the break flow rate and control the RCP [RCS] inventory. The PSA conservatively ignores operator backup following this I&C failure.

5.1.4.2. Medium Primary Break – PBM

5.1.4.2.1. Event Description

The initiating event "Medium Primary Break" is split into two sub-initiating events:

- PBM1-_AB, between 100 cm^2 < LOCA ≤ 180 cm^2.
- PBM2-_AB, between 45 cm^2 < LOCA ≤ 100 cm^2.

These are studied only for at-power states.

PBM1-_AB

The transient is similar to a Small Primary Break at-power but with a faster depressurisation and a greater energy release through the break.

Partial cooldown is not required because depressurisation of the primary circuit is provided by the break itself. The RCP [RCS] pressure decreases sufficiently to allow MHSI injection into the cold legs. At least one MHSI pump is required to provide sufficient makeup to the RCP [RCS].

The RIS [SIS] accumulators discharge cold water with the LHSI and MHSI trains injecting to keep the core completely covered.

While the MHSI flow rate is insufficient to compensate for the break flow rate, the RCP [RCS] inventory decreases. Subsequently the RCP [RCS] water inventory depends on the balance between safety injection flow rates (MHSI, accumulators, LHSI) and the break flow rate.

The RCP [RCS] pressure decreases sufficiently to allow LHSI injection into the cold legs without a manual fast cool-down. If all LHSI trains fail, two MHSI trains are required to match the break flow rate.

IRWST cooling is performed with one RIS-RA [LHSI/RHR] train or one EVU [CHRS] train.

PBM2-_AB

The transient is similar to a Small Primary Break in an at-power state but with a faster depressurisation and a greater energy release through the break.

Partial Cool-down is initiated to allow MHSI injection into the cold legs. Otherwise the RCP [RCS] is fed by the RCV [CVCS] with suction from IRWST until the pressure falls to the MHSI discharge pressure.

The RIS [SIS] accumulators discharge cold water to keep the core completely covered.

If the MHSI trains are unavailable, fast secondary cooldown is manually actuated to reduce the RCP [RCS] pressure sufficiently for LHSI injection into the cold legs.

IRWST cooling is performed with one RIS-RA [LHSI/RHR] train or one EVU [CHRS] train.

5.1.4.2.2. Functional Safety Requirements

PBM1-_AB

This section presents the safety functions which are challenged by a Medium Primary Break (100-180 cm^2) in at-power state:

- **Reactivity Control**: Reactivity control during the transient is provided by rod drop following the reactor trip signal.

  The consequences of failure of the rods to drop are not considered in this section. They are considered in section 5.10 of this sub-chapter on Anticipated Transient Without Scram.

- Removal of core decay heat and stored heat. This safety function is divided into:

  - **Residual Heat Removal:** Residual heat removal is provided by the loss of reactor coolant to the break. The associated energy is released into the containment.

  - **Long term cooling:** Heat is removed from the containment by the cooling chain: LHSI/Component Cooling Water System (RRI [CCWS])/Essential Service Water System (SEC [ESWS]). Cooling of the IRWST is performed by the LHSI. In the event of the unavailability of cooling with one LHSI train, cooling is carried out by the Containment Heat Removal System (EVU [CHRS]).

- **Reactor Coolant System integrity**: the initiating event breaches the RCP [RCS].

- **Reactor Coolant System inventory control**: RCP [RCS] inventory control is provided by the Medium and Low-Head Safety Injection systems. The RIS [SIS] accumulators, together with these systems, maintain the core completely covered.

  In the event of unavailability of all MHSI trains, the RCP [RCS] inventory cannot be restored within the required time window. This leads to core damage.

PBM2-_AB

This section identifies the safety functions which are challenged by Medium Primary Breaks (45-100 cm^2) in at-power states:

- **Reactivity Control**: Reactivity control in the transient is provided by rod drop following the reactor trip signal.

  The consequences of failure of the rods to drop are not considered in this section. They are considered in section 5.10 of this sub-chapter on the Anticipated Transients Without Scram.

- Removal of core decay heat and stored heat. This safety function is divided into:

  - **Residual Heat Removal**: Residual heat removal is provided primarily by the secondary side, by feeding the steam generators with water and removing the steam produced. The following alternatives are available:

- For feeding the SGs: the Startup and Shutdown System (AAD [SSS]). In the event of failure of this system, the Emergency Feedwater System (ASG [EFWS]) starts automatically on low low SG level.

- To remove steam from SGs: the Main Steam Bypass (GCT [MSB]) is available for steam dump to the condenser. The Main Steam Relief Valves (VDA [MSRT]) or the Main Steam Safety Valves are available for steam dump to atmosphere.

Note: The secondary system contributes to controlling the RCP [RCS] inventory function by depressurising the primary side using partial or fast cooldown.

- o **Long term cooling**: Cooling of the IRWST is performed using the LHSI. In the event of unavailability of cooling with one LHSI train, cooling is provided by the Containment Heat Removal System (EVU [CHRS]).

- **Reactor Coolant System integrity**: the initiating event breaches the RCP [RCS].

- **Reactor Coolant System inventory control**: RCP [RCS] inventory control is achieved by the Medium and Low-Head Safety Injection systems. The RIS [SIS] accumulators, together with these systems, keep the core completely covered.

Prior to the delivery of safety injection, the pressure in the RCP [RCS] needs to be decreased via the secondary side by:

- o Automatic opening of the VDA [MSRT] or GCT [MSB] for partial cooldown if MHSI is available. If partial cooldown fails, the RCV [CVCS] provides RCP [RCS] inventory control until the initiation of a fast secondary cooldown.

- o Manual opening of the VDA [MSRT] for fast secondary cooldown if MHSI is unavailable.

5.1.4.2.3. Detailed Results

PBM1-_AB

A “Medium Primary Break (100-180 cm^2)” occurring in an at-power state represents **1.1% of the Internal Event CDF, with a frequency of 6.02E-09/r.y.**

The table below lists the dominant accident sequence which represents almost 96% of the initiating event risk.

Initiating event	***Brief description of the accident sequence***	***Frequency (per reactor per year)***
PBM1-_AB	All MHSI trains fail due to Common Cause Failures or multiple single failures of pumps or check valves (i.e. 3 out of 3 MHSI trains with 1 train lost due to the initiating event).	5.8E-09

The following systems are important for Medium Primary Breaks (100-180 cm^2) in at-power states:

- **MHSI pumps**. These are required to mitigate the LOCA: they compensate for the break flow rate and control the RCP [RCS] inventory. MHSI is essential for the medium LOCA (between 100 and 180 cm²), because the break is not large enough to depressurise to the LHSI and accumulator pressure setpoint but is large enough to quickly drain the RCP [RCS]: consequently the time window available for performing fast secondary cooldown is not sufficient.

- **Essential Service Water System (SEC [ESWS])** and **Component Cooling Water System (RRI [CCWS])**. These support systems are part of the safety related Cooling Chain. They are important because they cool the motors of the MHSI pumps.

PBM2-_AB

A “Medium Primary Break (45-100 cm^2)” in an at-power state represents **0.6% of the Internal Event CDF, with a frequency of 3.18E-09/r.y.**

The following table lists the dominant accident sequence which represents 97% of the initiating event risk.

Initiating event	***Brief description of the accident sequence***	***Frequency (per reactor per year)***
PBM2-_AB	All MHSI trains are inoperable due to Common Cause Failures or multiple single failures of pumps or check valves (i.e. 3 out of 3 MHSI trains; 1 train is lost due to the initiating event) **and** the operator fails to perform the fast secondary cooldown in 15 minutes.	3.1E-09

The following systems are important in the protection against Medium Primary Breaks (45-100 cm^2) during at-power states:

- **MHSI pumps**. These are required to mitigate the LOCA: they compensate for the break flow rate and control the RCP [RCS] inventory.

- **Essential Service Water System (SEC [ESWS]) and Component Cooling Water System (RRI [CCWS]).** These support systems are part of the safety related Cooling Chain. They are important because they cool the motors of the MHSI pumps.

The following operator action is important in the protection against the Medium Primary Break (45-100 cm^2) during at-power states:

- The **operator initiates a Fast Secondary Cooldown**. This action is required in the event of the failure of the MHSI. The effect is to decrease the RCP [RCS] pressure sufficiently to allow LHSI injection into the cold legs.

5.1.4.3. Large Primary Break – PBL

5.1.4.3.1. Event Description

The initiating event "Large Primary Break" corresponds to the spectrum 180 cm^2 < LOCA ≤ 830 cm^2. It is studied only for at-power states.

The transient is very similar to the Medium Primary Break (100-180 cm^2) in an at-power state (PBM1-_AB). The only difference is that the RCP [RCS] depressurises quickly down to the LHSI and accumulator pressure setpoint.

5.1.4.3.2. Required Safety Functions

This section presents the safety functions which are challenged by the Large Primary Break in a power state:

- **Reactivity Control**: Reactivity control during the transient is provided by rod drop following the reactor trip signal.

  The consequences of the failure of the rods to drop are not considered in this section. They are considered in the section 5.10 of this sub-chapter on Anticipated Transients Without Scram.

- Removal of core decay heat and stored heat. This safety function is divided into:

  - **Residual Heat Removal**: Residual heat removal is provided by the loss of reactor coolant to the break. The associated energy is discharged to the containment.

  - **Long term cooling**: Heat is removed from the containment by the RRI [CCWS]/SEC [ESWS] cooling chain. Cooling of the IRWST is performed by the LHSI. In the event of the unavailability of cooling by at least one LHSI train, cooling is provided by the Containment Heat Removal System (EVU [CHRS]) (1 out of 2 trains required).

- **Reactor Coolant System integrity**: the initiating event breaches the RCP [RCS].

- **Reactor Coolant System inventory control**: RCP [RCS] inventory control is provided by the Medium and Low-Head Safety Injection systems. The RIS [SIS] accumulators support these systems in keeping the core completely covered.

5.1.4.3.3. Detailed Results

The "Large Primary Break (180-830 cm^2)" in at-power states **results in negligible consequences (CDF=5.85E-11/r.y).**

5.1.4.4. 2A-LOCA – PBL-2A-_AB

5.1.4.4.1. Event Description

The initiating event "2A-LOCA" corresponds to a double-ended guillotine break of a main coolant line. It is studied only for at-power states.

The transient is very similar to the Large Primary Break (100-180 cm^2) in an at-power state (PBL-_AB). In the absence of support studies for this break size, assumptions on success criteria are made. These assumptions are judged conservative based on Large Primary Break success criteria.

5.1.4.4.2. Required Safety Functions

This section presents the safety functions which are challenged by the Large Primary Break in a power state:

- **Reactivity Control**: Reactivity control during the transient is provided by rod drop following the reactor trip signal.

  The consequences of the failure of the rods to drop are not considered in this section. They are considered in the section 5.10 of this sub-chapter on Anticipated Transients Without Scram.

- Removal of core decay heat and stored heat. This safety function is divided into:

  - **Residual Heat Removal**: Residual heat removal is provided by the loss of reactor coolant to the break. The associated energy is discharged to the containment.

  - **Long term cooling**: Heat is removed from the containment by the RRI [CCWS]/SEC [ESWS] cooling chain. Cooling of the IRWST is performed by the LHSI. Should cooling by at least one LHSI train be unavailable, cooling is provided by the Containment Heat Removal System (EVU [CHRS]) (1 out of 2 trains required).

- **Reactor Coolant System integrity**: the initiating event breaches the RCP [RCS].

- **Reactor Coolant System inventory control**: RCP [RCS] inventory control is provided by the Medium and Low Head Safety Injection systems. The RIS [SIS] accumulators support these systems in keeping the core completely covered.
  The success criterion 2 out of 3 MHSI, 2 out of 3 LHSI and 3 out of 3 RIS [SIS] accumulators is likely to be conservative.

5.1.4.4.3. Detailed Results

The “2A-LOCA” in at-power states represents **0.2% of the Internal Event CDF, with a frequency of 1.28E-09/r.y.**

The following table lists the dominant accident sequence which represents almost 88% of the initiating event risk.

Initiating event	*Brief description of the accident sequence*	*Frequency (per reactor per year)*
PBL-2A_AB	2 out of 3 MHSI trains (1 train is lost due to the initiating event) are inoperable due to Common Cause Failures (CCF) or multiple single failures on pumps or check valves.	1.1E-9

The following systems are important in the protection against 2A-LOCA during at-power states:

- **LHSI pumps**. 2 out of 3 trains available are required to mitigate the 2A-LOCA: they compensate for the break flow rate and control the RCP [RCS] inventory.
- **MHSI pumps**. 2 out of 3 trains available are required to mitigate the 2A-LOCA: they compensate for the break flow rate and control the RCP [RCS] inventory.

5.1.4.5. Reactor Pressure Vessel Failure – RPV_F

5.1.4.5.1. Event Description

The initiating event “reactor pressure vessel failure” corresponds to a rupture of the reactor pressure vessel without any possible recovery of the core. It is studied for at-power states and shutdown states (brittle fracture).

This transient is not analysed in the frame of the Level 1 Probabilistic Safety Assessment as no recovery is considered.

5.1.4.5.2. Detailed Results

The RPV failure leads directly to unacceptable consequences, thus the core damage frequency considered in the UK EPR PSA is the same as the initiating event frequency: {CCI} [a].

5.2. INTERFACING SYSTEM LOCA - V-LOCA

5.2.1. Group Description

A V-LOCA is a break on a system connected to the Reactor Coolant System (RCP [RCS]) and partly located outside the containment, which may induce a loss of coolant accident and draining of the IRWST outside the containment if the break is not isolated.

This type of transient involves containment bypass via auxiliary systems connected to the Reactor Coolant System.

The following auxiliary systems are connected to the Reactor Coolant System:

- Chemical and Volume Control System (RCV [CVCS]).
- Safety Injection System (RIS [SIS]).
- Extra Borating System (RBS [EBS]).
- Nuclear Sampling System (REN [NSS]).
- Nuclear Vent and Drain System (RPE [NVDS]).
- Component Cooling Water System (RRI [CCWS]) via the reactor coolant pumps thermal barrier.

The V-LOCA scenario caused by the Containment Heat Removal System (EVU [CHRS]), causing draining of the IRWST is also studied.

Size of the V-LOCA breaks

All breaks which cannot be compensated for by one RCV [CVCS] charging pump, a flow rate > 36 t/h, are addressed, except for:

- Breaks located inside containment as they are standard LOCAs and not V-LOCAs.
- SGTR initiating events as they are studied in the SGTR accident group. This is discussed in section 5.4 of this sub-chapter.

For breaches with flow rates of < 36 t/h, only V-LOCAs in the RIS-RA [LHSI/RHR] trains are addressed.

V-LOCA scenarios are analysed for at-power states as well as for shutdown states during which the Low-Head Safety Injection (LHSI) trains are operating in RHR mode, states Ca, Cb, D and E. Consequently, the following initiating events are considered in the group [Ref-1]:

- V-LOCA during at-power states A and B (PBV_AB).
- Small V-LOCAs on the RIS-RA [LHSI/RHR] during shutdown states Ca, Cb, D and E (PBV1-_CA, PBV1-_CB, PBV1-_D-, PBV1-_E-).
- Significant V-LOCAs on the RIS-RA [LHSI/RHR] during shutdown states Ca, Cb, D and E (PBV2-_CA, PBV2-_CB, PBV2-_D-, PBV2-_E-).

The definitions and frequencies of the initiating events are given in section 4 of this sub-chapter.

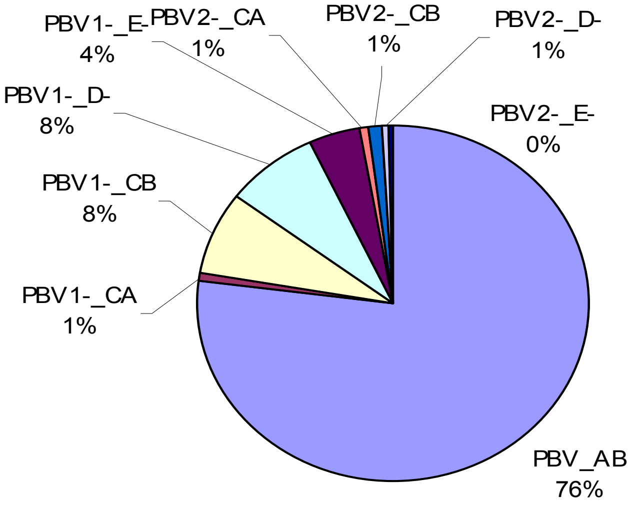
5.2.2. Results

The contribution of the V-LOCA group to the **Core Damage Frequency is 4.80E-09/r.y**, which represents **0.9% of the Internal Event CDF.**

The CDF for each V-LOCA initiating event within the group is shown in the following table:

Initiating Event	IE frequency (/y)	CDF (/r.y)
PBV_AB	{CCI}[a]	{CCI}[a]
PBV1-_CA	{CCI}[a]	3.38E-11
PBV1-_CB	{CCI}[a]	3.65E-10
PBV1-_D-	{CCI}[a]	3.76E-10
PBV1-_E-	{CCI}[a]	1.94E-10
PBV2-_CA	{CCI}[a]	4.31E-11
PBV2-_CB	{CCI}[a]	4.77E-11
PBV2-_D-	{CCI}[a]	2.90E-11
PBV2-_E-	{CCI}[a]	1.37E-11
total		4.80E-09

The relative contribution of each V-LOCA initiating event within the group is given below:



5.2.3. Dominant Accident Sequences Analysis

The following table lists the main accident sequences of the V-LOCA group. Each accident sequence corresponds to one or a group of Minimal CutSets (MCS). The main accident sequences considered in the table below represent 66% of the group CDF.

Initiating event	*Brief description of the accident sequence*	*Frequency (per reactor per year)*
PBV_AB	A Leak in a reactor coolant pump thermal barrier (Reactor Coolant System side) located upstream the thermal barrier. This flows into the RRI [CCWS]. The lines of defence to prevent V-LOCA scenarios are the Tubes of the thermal barrier, 1 lift check valve, 1 motor operated valve automatically closed on high temperature signal.	{CCI}[a]
PBV_AB	The scenario begins by a complex sequence of an initiating event requiring the EVU [CHRS] operation **then** a leakage on the main line or an external leakage of a component located on the main EVU line occurs. The lines of defence to prevent V-LOCA scenarios are the EVU [CHRS] main line and its components and 1 manually closed motor operated valve.	{CCI}[a]
PBV_AB	During reactor states A to Ca the reactor coolant pumps are in operation and the RCV [CVCS] maintains the pumps leak tightness. The lines of defence to prevent V-LOCA coming from the RCV seal injection are the RCV [CVCS] charging line and seal injection line and 3 check valves (2 lift check valves and 1 swing check valve).	{CCI}[a]

5.2.4. Initiating Events Analysis

Sub-section 5.2.4.1 of this sub-chapter analyses the lines of defence available on the design of each interfacing system to prevent V-LOCA scenarios during at-power states. Sub-section 5.2.4.2 of this sub-chapter analyses V-LOCA involving the failure of the RIS-RA [LHSI/RHR] trains connected to the RCP [RCS] when this system is in operation during the shutdown states.

5.2.4.1. V-LOCA in at-power states (PBV_AB)

For V-LOCA in at-power states and hot standby (PBV_AB), it is conservatively assumed that the initiating event leads directly to core damage.

5.2.4.1.1. V-LOCA on RIS-RA [LHSI/RHR]

Two types of V-LOCA scenarios can be identified, depending on the reactor states. During at-power state and hot standby states (A and B) the hot leg suction lines and the cold leg injection lines are isolated from the RCP [RCS]. The temperature and pressure in the RCP [RCS] are high.

The RIS-RA [LHSI/RHR] system is in stand-by.

The lines of defence to prevent V-LOCA scenarios are:

- Cold leg injection side
  - 3 check valves in series with a diverse technology for the second check valve.
  - Permanent monitoring of the temperature and the pressure between the first and the second isolation check valves enabling the detection and locating of the leak.
- Hot leg suction side
  - 2 motor operated valves inside the containment and 1 motor operated outside the containment.
  - The pipe located between the containment and the third motor operated valves is designed to withstand the RCP [RCS] thermal hydraulic conditions.
  - Permanent monitoring of the temperature and the pressure between the first and the second motor operated isolation valves enabling the detection and the locating of the leak.

The frequency of this V-LOCA initiating event during at-power states is {CCI} [a]

5.2.4.1.2. V-LOCA on RCV [CVCS]

Prevention of V-LOCA scenarios is provided by components located inside the containment. For all initiators in reactor states Cb to E, the primary pressure is 1 bar and there is no risk of a V-LOCA. As a consequence, RCV [CVCS] initiators are not analysed for reactor states Cb to E.

The list of the potential V-LOCA scenarios is:

- Tube(s) rupture of a HP cooler on the RCV [CVCS] letdown line.
- Spurious full opening of the pressure-reduction valve.
- Rupture of the RCV [CVCS] letdown line, outside containment.
- Rupture/leakage of the charging line outside the containment.

5.2.4.1.2.1. Tube(s) rupture of a HP cooler on the RCV [CVCS] letdown line

The lines of defence to prevent V-LOCA scenarios are:

- HP cooler tubes.
- 2 motor operated valves automatically isolating the letdown line.
- 2 motor operated valves for manual isolation of the affected HP cooler.
- Monitoring to detect and to locate the break.

The frequency of this V-LOCA initiating event during at-power states is negligible.

5.2.4.1.2.2. Spurious full opening of the pressure-reduction valve

The lines of defence to prevent V-LOCA scenarios are:

- 1 safety valve designed to maintain the pressure below 1.2 MPa.
- 2 motor operated valves automatically isolating the letdown line.
- 2 manually actuated motor operated valves on HP cooler 1 and HP cooler 2 to isolate the leak path.
- Monitoring to detect and to locate the break.

The frequency of this V-LOCA initiating event during at-power states is equal to {CCI} [a] and is negligible for state Ca.

5.2.4.1.2.3. Rupture on the RCV [CVCS] letdown line, outside containment

The lines of defence to prevent V-LOCA scenarios are:

- 2 motor operated valves automatically isolating the letdown line.
- 2 manually actuated motor operated valves on HP cooler 1 and HP cooler 2 to isolate the leak path.
- 1 manually actuated containment isolation valve inside the containment to isolate the leak path.
- Monitoring to detect and to locate the break.

This scenario is screened out because of the large number of lines of defence.

5.2.4.1.2.4. Rupture/leakage on the charging line outside the containment

<u>V-LOCA on the charging lines</u>

The lines of defence to prevent V-LOCA scenarios are:

- RCV [CVCS] charging lines.
- 3 check valves in series.
- 1 motor operated valve automatically isolating the charging line in the event of reverse flow in the charging line.
- 3 motor operated valves manually closed by the operator.
- Monitoring to detect and to locate the break.

The frequency of this V-LOCA initiating event during at-power states is {CCI} [a] and is negligible for state Ca.

V-LOCA on the main coolant pumps

During reactor states A to Ca the main coolant pumps are in operation and the RCV [CVCS] provides the pumps' leak tightness.

The lines of defence to prevent V-LOCA scenarios are:

- RCV [CVCS] charging line and seal injection line.
- 3 check valves (2 lift check valves and 1 swing check valve).

The frequency of this V-LOCA initiating event during at-power states is {CCI} [a] and is negligible for state Ca.

5.2.4.1.3. V-LOCA on Extra Borating System RBS [EBS]

The prevention of V-LOCA scenarios is achieved by components inside the containment: namely the lift ball check-valves and the piping between these check-valves and the containment.

As the primary pressure is equal to 1 bar in state Cb to E, the RBS [EBS] initiators are analysed only in reactor states A to Ca.

The list of the potential V-LOCA scenarios is:

- RBS [EBS] in standby and failure of the lines of defence inside the containment leading to the pressurisation of the RBS [EBS] outside the containment and the following:
  - Failure of the lift ball check-valves and consequent piping rupture upstream of the pump (scenario 1).
  - Failure of the pipe or safety valve downstream of the RBS [EBS] pump (scenario 2).
- RBS [EBS] in operation and failure of the lines of defence inside the containment after normal shutdown causing the pressurisation of RBS [EBS] outside the containment and the following:
  - Failure of the lift ball check-valves upstream of the RBS [EBS] pump (scenario 3).
  - Failure of the pipe or safety valve downstream of the RBS [EBS] pump (scenario 4).

5.2.4.1.3.1. EBS in standby

Scenario 1

The lines of defence to prevent V-LOCA scenarios are:

- 2 check valves.
- 1 normally-closed motor operated valve.

- 2 lift ball check valves on each piston of the RBS [EBS] pump.
- Monitoring to detect and to locate the break.

The frequency of this V-LOCA initiating event during at-power states is {CCI} [a]. It is negligible for state Ca.

Scenario 2

The lines of defence to prevent V-LOCA scenarios are:

- 2 check valves.
- 1 normally closed motor operated valve.
- The RBS [EBS] injection line.
- Monitoring to detect and to locate the break.

The frequency of this V-LOCA initiating event during at-power states is negligible.

5.2.4.1.3.2. RBS [EBS] in operation

Scenario 3

The lines of defence to prevent V-LOCA scenarios are:

- 2 check valves with a diverse technology.
- 2 lift ball check valves on each piston of the RBS [EBS] pump.
- Monitoring to detect and to locate the break.

cy of this V-LOCA initiating event during at-power states is negligible {CCI removed} [a]. It is much lower for state Ca.

Scenario 4

The lines of defence to prevent V-LOCA scenarios are:

- 2 check valves with a diverse technology.
- The RBS [EBS] injection line.
- Monitoring to detect and to locate the break.

The frequency of this V-LOCA initiating event during at-power states is equal to {CCI} [a]. It is negligible for state Ca.

5.2.4.1.4. V-LOCA on Nuclear Sampling System REN [NSS]

The Nuclear Sampling System REN [NSS] is connected to the RCP [RCS] on the hot legs of reactor coolant loops 1 and 3 and the pressuriser steam and liquid phase.

The sampling lines are permanently open. Each sampling line is provided with at least two isolation valves in series inside the containment and one isolation valve outside the containment. The diameter of the pipe outside the containment is very small (DN8). A break of a nuclear sampling line results only in leakages which can be compensated for by the RCV [CVCS]. Such leaks are not considered as a V-LOCA.

5.2.4.1.5. V-LOCA on Nuclear Vents and Drains System RPE [NVDS]

The connections of the Nuclear Vents and Drain System to Reactor Coolant System boundaries are:

- Pressuriser venting line.
- Reactor vessel vent line.
- Reactor coolant system seals.

Permanent connections to systems of high design pressure are protected by means of flow restrictors and safety valves to reduce the high pressure to the permissible pressure of the drain system.

There is no identified V-LOCA scenario.

5.2.4.1.6. V-LOCA on Component Cooling Water System (RRI) [CCWS]

The RRI [CCWS] is not directly connected to the RCP [RCS] but its heat exchangers belong to the following systems directly connected to the RCP [RCS]:

- Low-Head Safety Injection system RIS-RA [LHSI/RHR].
- Chemical and Volume Control System RCV [CVCS].
- Thermal barrier of main coolant pump.

All reactor coolant pumps are stopped from part of state Ca to state E. After shutdown of the last reactor coolant pump, all the thermal barriers are isolated. Consequently, the only reactor states considered are A to Ca. A leakage in a reactor coolant pump thermal barrier (Reactor Coolant System side) flows into the RRI [CCWS].

Two initiators are studied, depending on whether the location of the rupture outside containment is upstream or downstream of the thermal barrier.

Upstream of the thermal barrier

The lines of defence to prevent V-LOCA scenarios are:

- Tubes of the thermal barrier.
- 1 lift check valve.
- 1 motor operated valve automatically closed on a high temperature signal.

The frequency of this V-LOCA initiating event during at-power states is equal to {CCI} [a]. It is very small for state Ca.

Downstream of the thermal barrier

The lines of defence to prevent V-LOCA scenarios are:

- Tubes of the thermal barrier.
- 1 solenoid valve automatically closed on a high temperature signal.
- A manual throttle valve to limit the flow rate.

The frequency of this V-LOCA initiating event during at-power states is equal to {CCI} ^{a}. It is negligible for state Ca.

5.2.4.1.7. V-LOCA on Containment Heat Removal System EVU [CHRS]

The following section presents the V-LOCA initiators which can lead to draining of the IRWST via the EVU [CHRS]. It is assumed that the draining of the IRWST leads directly to the core damage.

Special design measures have been taken on the EVU [CHRS] to minimise the risk of breaks and leaks on the pipe work and important components:

V-LOCA sequences can occur only if there is a breach in the RCP [RCS] leading to a loss of coolant from the IRWST. In the following discussions these sequences are referred to as "complex PSA sequences".

The list of the potential V-LOCA scenarios is:

- EVU [CHRS] in standby during complex PSA sequences and loss of IRWST water inventory outside the containment.
- EVU [CHRS] in operation to cool the IRWST during complex sequences and loss of IRWST water inventory outside the containment.
    - EVU [CHRS] heat exchanger tube(s) rupture.
    - Rupture or leakage of the EVU [CHRS] main line or components.

5.2.4.1.7.1. EVU [CHRS] in standby mode

Special design measures have been taken on the EVU [CHRS] to minimise the risk of breaks and leaks on pipes and important components. No rupture or external leakage of components on the main circuit is assumed during standby mode.

The likelihood of emptying the IRWST via the EVU [CHRS] during the stand by period is assumed to be negligible.

5.2.4.1.7.2. EVU [CHRS] in operation

Scenario 1

The scenario is initiated by the rupture of tube(s) inside the heat exchanger of the main cooling circuit during a complex sequence.

The pressure is controlled in the intermediate cooling circuit, to maintain a positive differential to the main cooling circuit pressure ($P_{\text{intermediate circuit}} > P_{\text{main circuit}}$).

Consequently, unless there are additional failures, the risk of draining the IRWST in the event of tube(s) rupture in the heat exchanger is low.

Scenario 2

The scenario begins with a complex sequence of an initiating event requiring EVU [CHRS] operation. A rupture on the EVU [CHRS] main line then occurs. The leakage is detected by "high sump level" in the sumps located in the EVU [CHRS] room.

The lines of defence to prevent V-LOCA scenarios are:

- EVU [CHRS] main line.
- 1 manually closed motor operated valve.

The frequency of this V-LOCA initiating event during at-power states is {CCI} [a].

Scenario 3

Same as scenario 2 but the failure of the EVU [CHRS] is due to a leak on the main pipe work or from a component in it.

The lines of defence to prevent V-LOCA scenarios are:

- EVU [CHRS] main pipe work and the components.
- 1 manually closed motor operated valve.

The frequency of this V-LOCA initiating event during at-power states is {CCI} [a]. As it is much more likely that the EVU [CHRS] would be put in service from at-power states than from shutdown states, the frequency of this V-LOCA initiating event during shutdown states is negligible.

5.2.4.1.8. Conclusion

The global probability of core damage due to a V-LOCA during at-power states (states A and B) is {CCI} [a].

5.2.4.2. V-LOCA during shutdown states

Only V-LOCA characterised by the failure of the RIS-RA [LHSI/RHR] trains connected to the RCP [RCS] are analysed:

- The small V-LOCA on RIS-RA: PBV1-_CA, PBV1-_CB, PBV1-_D-, PBV1-_E-.
- The significant V-LOCA on RIS-RA: PBV2-_CA, PBV2-_CB, PBV2-_D-, PBV2-_E-.

5.2.4.2.1. Event Description

Small V-LOCA (PBV1)

The initiating event “Small V-LOCA on LHSIS/RHR” during shutdown states corresponds to a V-LOCA caused by a small leakage on the hot leg suction lines or on the injection lines outside the containment from 5 to 20 cm².

The consequences of a small V-LOCA on the RIS-RA [LHSI/RHR] trains connected to the RCP [RCS] differ, depending on the reactor state.

For state Ca, the leak leads to a loss of primary water inventory, to an increase of the sump level and to an increase in the auxiliary safeguard building inner pressure outside the containment of the affected train. Due to the initial primary water inventory in this state, the high sump level signal and the high auxiliary safeguard building pressure signal, which actuates isolation of the affected train, will be reached before any other signal. Due to the small break size the RCP [RCS] hot legs remain in sub-cooling conditions. If the automatic isolation fails the water level and pressure decrease in the RCP [RCS]. In this case the isolation is performed manually. The Medium-Head Safety Injection is activated following a low delta-Psat signal and the RHR trains in operation are tripped. If the MHSI fails, the Low-Head Safety Injection is started manually. If the primary RHR with LHSI trains fails, the Residual Heat Removal from the secondary side is initiated on high SG-pressure and low SG-level.

In states Cb and D, the initial primary water inventory corresponds to 3/4-loop. The loss of primary water inventory through the break outside containment leads to the automatic actuation of the MHSI trains on low RCP [RCS] level. The RHR trains in operation are tripped automatically. It is assumed that the safeguard building sump level signal high, which performs the automatic isolation of the affected train, is reached after the actuation of the MHSI trains and the LHSI pumps trip, for the pumps operating in RHR mode. The automatic actuation of the MHSI trains or the manual actuation of the LHSI trains in injection mode allows recovery of the RIS-RA [LHSI/RHR] operation in the long term. For state Cb, the PSA considers the Residual Heat Removal performed by the secondary side.

For state E, in the event of successful isolation, no additional makeup is needed. When the Reactor pool is flooded, the water inventory is large enough to prevent the RHR trip even with a small leak lasting several hours.

Significant V-LOCA (PBV2)

The initiating event “Significant V-LOCA on LHSIS/RHR” during shutdown states corresponds to a V-LOCA caused by a significant leak due to a break (leakage or rupture) of the hot leg suction lines or on the injection lines outside the containment. The break is assumed to range from 20 cm² up to a double guillotine break of a RHR line.

The consequences of a significant V-LOCA on the RIS-RA [LHSI/RHR] trains connected to the RCP [RCS] differ, depending on the reactor state.

In state Ca, the pressuriser level decrease is rapid. Saturation conditions are reached in the RCP [RCS] hot legs. In these conditions, injection into the RCP [RCS] is rapidly required. Injection is performed by the MHSI trains following a low delta-Psat signal or by manual actuation of the LHSI trains in injection mode following trip of the RHR trains in operation. If automatic isolation is successful, the RCP [RCS] cooling could be restored following successful safety injection by:

- Either the LHSI trains in RHR mode.
- Or from the secondary side, initiated automatically on high SG-pressure and low SG-level.

For state Cb, the consequences of a significant V-LOCA are similar to those of a significant V-LOCA during state Ca. Only the Safety injection signal changes: “low delta-Psat” is replaced by “low RCP [RCS] level”.

For state D, the consequences of a significant V-LOCA are similar to those of a significant V-LOCA during state Cb. The PSA does not consider Residual Heat Removal from the secondary side for this plant state.

For state E, due to the size of the leak, the reactor cavity draining is quite rapid and is complete in less than 90 minutes. If isolation is performed within 90 minutes, the RIS-RA [LHSI/RHR] is maintained in operation.

5.2.4.2.2. Functional Safety Requirements

Small V-LOCA (PBV1)

This section presents the safety functions which are challenged by a Small V-LOCA during shutdown states:

- **Reactivity Control:** Reactivity control is not challenged by the transient.
- Remove core decay heat and stored heat. This safety function is divided into:
  - o **Residual Heat Removal**: Primary circuit heat removal can be performed by the secondary side with 1 out of 4 steam generators in states Ca and Cb. It can be performed by the remaining Low-Head Safety Injection trains in RHR mode in all states. The RHR operation of the LHSI pumps is supported by the automatic actuation of Medium-Head Safety Injection pumps.
    For state E, if isolation is successful, no additional makeup by the MHSI pumps is needed. If the automatic isolation fails, the water inventory remains large enough after manual isolation to match the required steaming without makeup.

    For state Ca and Cb, an alternative is the primary Feed and Bleed with feed by the Safety Injection System and the opening of the primary depressurisation valves or the pressuriser safety valves..
  - o **Long term cooling**: As the PSA does not consider Feed and Bleed, the IRWST temperature remains low. There is no specific feature for long term cooling in case of small V-LOCA.

- **Reactor Coolant System integrity**: The initiating event breaches the RCP [RCS]. However manual or automatic isolation of the leak or break on the affected RIS-RA [LHSI/RHR] train is possible. In the event of the failure of the automatic actions, the operator can perform a manual isolation from the main control room. The failure of automatic and manual isolation of the leak or break is assumed to lead to unacceptable consequences with containment bypass.

- **Reactor Coolant System inventory control**: For states Ca to D, the makeup function is performed either automatically by the Medium-Head Safety Injection or manually by starting the remaining Low-Head Safety Injection trains in injection mode. In state E, after successful isolation of the break, the inventory in the reactor cavity is large enough to prevent core damage for a period of more than 24 hours without makeup functions operating.

Significant V-LOCA (PBV2)

The safety functions challenged by a significant V-LOCA during shutdown states are the same as those for a small V-LOCA.

5.2.4.2.3. Detailed Results

Small V-LOCA (PBV1)

A Small V-LOCA in shutdown states represents less than **0.2% of the Internal Event CDF with a frequency of 9.70E-10/r.y.**

The following table lists the dominant accident sequences. Each accident sequence corresponds to one or a group of MCS. The main accident sequences considered in the table below represent 80% of the initiating event risk.

Initiating event	***Brief description of the accident sequence***	***Frequency (per reactor per year)***
PBV1-_CB	All RRI/SEC [CCWS/ESWS] pumps fail to run due to a CCF. Consequently, the MHSI and LHSI pumps are unavailable for injection due to the failure of their cooling and the LHSI trains are inoperable in RHR mode due to failure of the cooling chain. Conservatively EVU [CHRS] is not claimed.	3.3E-10
PBV1-_D-	All RRI/SEC [CCWS/ESWS] pumps fail to run due to a CCF. Consequently, the MHSI and LHSI pumps are unavailable for injection due to the failure of their cooling and the LHSI trains are inoperable in RHR mode due to failure of the cooling chain. Conservatively EVU [CHRS] is not claimed.	1.9E-10
PBV1-_E-	Automatic isolation of the affected train is not achieved due to a I&C failure and the manual initiation of the Residual Heat Removal by LHSI trains fails due to a I&C failure.	1.3E-10
PBV1-_D-	All MHSI pumps fail to run due to a CCF and the operator fails to initiate the primary water makeup by LHSI trains.	1.3E-10

The following systems are important in the protection against Small V-LOCA in shutdown states:

- **MHSI pumps**. These systems are required to mitigate the V-LOCA: they compensate for the break flow and control the RCP [RCS] inventory.

- **Essential Service Water System (SEC [ESWS]) and Component Cooling Water System (RRI [CCWS])**. These support systems are part of the safety related Cooling Chain. They are important because they provide heat removal from the Reactor Coolant System and they participate in the cooling of the safety injection pump motors.

The following I&C signal and platform are important in the protection against Small V-LOCA in shutdown states:

- **PS signal “High sump level outside containment”**. The failure of this signal prevents the automatic isolation of the affected train. The PSA considers operator back-up after this I&C failure.

- **SPPA-T2000**. This platform is required to manually initiate the Residual Heat Removal by one LHSI train.

The following operator action is important in the protection against Small V-LOCA in shutdown states:

- **Initiation of the primary water make up by LHSI trains.** This manual action is important because injection is performed either automatically by the MHSI trains or by manual actuation of the LHSI trains in injection mode following trip of the RHR trains in operation.

Significant V-LOCA (PBV2)

A Significant V-LOCA in shutdown states represents **0.03% of the Internal Event CDF with a frequency of 1.34E-10/r.y.**

The following table lists the dominant accident sequence which represents 54% of the initiating event risk.

Initiating event	*Brief description of the accidental sequence*	*Frequency (per reactor per year)*
PBV2-_CB	All RRI/SEC [CCWS/ESWS] pumps fail to run due to a CCF. Consequently, the MHSI and LHSI pumps are unavailable for injection due to the failure of their cooling and the LHSI trains are inoperable in RHR mode due to the failure of the cooling chain. Conservatively EVU [CHRS] is not claimed.	2.2E-11
PBV2-_CA	All RRI/SEC [CCWS/ESWS] pumps fail to run due to a CCF. Consequently, the MHSI and LHSI pumps are unavailable for injection due to the failure of their cooling and the LHSI trains are inoperable in RHR mode due to the failure of the cooling chain. Conservatively EVU [CHRS] is not claimed.	1.6E-11

Initiating event	***Brief description of the accidental sequence***	***Frequency (per reactor per year)***
PBV2-_D-	All RRI/SEC [CCWS/ESWS] pumps fail to run due to a CCF. Consequently, the MHSI and LHSI pumps are unavailable for injection due to the failure of their cooling and the LHSI trains are inoperable in RHR mode due to the failure of the cooling chain. Conservatively EVU [CHRS] is not claimed.	1.2E-11
PBV2-_E-	Automatic isolation of the affected train is not achieved due to a I&C failure and the manual isolation of the affected train fails due to a I&C failure.	8.7E-12
PBV2-_D-	All MHSI pumps fail to run due to a CCF and the operator fails to initiate the primary water makeup by LHSI trains.	8.6E-12
PBV2-_CA	Automatic isolation of the affected train is not achieved and the MHSI pumps do not start automatically due to a I&C failure and the operator fails to initiate the primary water makeup by LHSI or MHSI trains.	5.6E-12

The following systems are important in the protection against a Significant V-LOCA in shutdown states:

- **Essential Service Water System (SEC [ESWS]) and Component Cooling Water System (RRI [CCWS])**. These support systems are part of the safety related Cooling Chain. They are important because they provide the heat removal from the Reactor Coolant System and they participate in the cooling of the safety injection pump motors.

- **MHSI pumps**. These systems are required to mitigate the V-LOCA: they compensate for the break flow and control the RCP [RCS] inventory.

The following I&C signals/platform are important in the protection against Significant V-LOCA in shutdown states:

- **PS signals "High sump level or high sump pressure outside containment"**. The failure of these signals prevents the automatic isolation of the affected train. The PSA considers operator back-up after this I&C failure.

- **SPPA-T2000**. This platform is required to manually isolate the affected train in case of failure of the automatic isolation and to manually initiate Residual Heat Removal by LHSI trains.

- **PS signal "Low delta-Psat"**. The failure of this signal prevents the MHSI pumps from starting and the RHR pumps in operation from being realigned to inject into the cold legs in LHSI mode. Consequently the MHSI and LHSI pumps are unavailable to compensate for the break flow rate and control the RCP [RCS] inventory. Manual start of the MHSI pumps is credited if this PS signal fails.

The following operator action is important in the protection against Significant V-LOCA in shutdown states:

- **Initiation of the primary water make up by LHSI trains.** This manual action is important because injection is performed either automatically by the MHSI trains or by manual actuation of the LHSI trains in injection mode following trip of the RHR trains in operation.

5.3 SECONDARY BREAKS

5.3.1. Group Description

The secondary breaks group covers events equivalent to steam line breaks of different sizes, located between the exit of the Steam Generators (SG) and the turbine.

The consequences of a steam line break can be divided in two phases:

- Immediately after the break, depressurisation of the SGs causes a significant increase in steam flow from the SGs. This steam flow causes a fast, uncontrolled cool down of the Reactor Coolant System (RCP [RCS]) and potentially an increase in reactivity. Following this short overcooling transient, the SGs connected to the break may be drained by the blow down leading to degraded secondary heat removal conditions.

- On the secondary side, protection is provided by closure of the MSIVs to halt the uncontrolled steam flow. If necessary, the automatic and manual isolation of the depressurised SG(s) feed line(s) is also performed. On the reactor coolant side, protection consists of providing sufficient injection of negative reactivity with a reactor trip and, if necessary, boration of the RCP [RCS] using the Medium Head Safety Injection system (MHSI) and the accumulators.

The following initiating events are considered in the group:

- Large steam line break downstream of a Main Steam Isolation Valves (MSIV) outside the containment during at-power state A or intermediate shutdown B - SLB_LO_AB,

- Large steam line break upstream of a MSIV inside the containment during at-power state A or intermediate shutdown B - SLB_LI_AB,

- Small steam line break upstream of a MSIV outside the containment (such as spurious opening of MSRT or stuck open MSSV) in at-power state A or intermediate shutdown B - SLB_SO_AB.

The definition and frequencies of the initiating events are given in section 4 of this sub-chapter. The frequencies are tabulated in the next section.

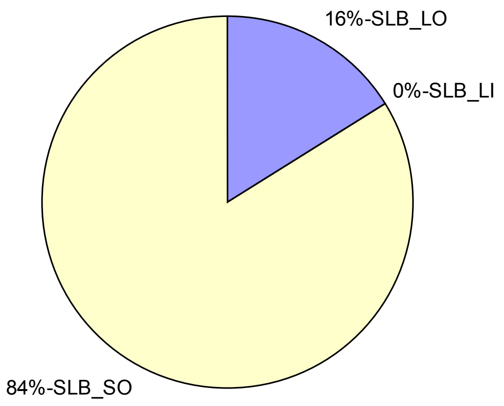
5.3.2. Results

The contribution of the secondary breaks group to the **Internal Event Core Damage Frequency is 1.3E-8/r.y** which represents **2.5% of the Internal Event CDF**.

The CDF for each secondary break initiating event within the group is shown in the following table:

Initiating Event	IE frequency (/y)	CDF (/r.y)
SLB_LO_AB	{CCI} [a]	2.1E-9
SLB_LI_AB	1.30E-06	9.2E-12
SLB_SO_AB	{CCI} [a]	1.1E-8
total		1.3E-8

The relative contribution of each secondary break initiating event within the group is given below:



A small steam line break poses less of a safety challenge than a large break because the lower steam flow causes a slower uncontrolled cooldown.

However, the group CDF is dominated by the small steam line breaks. This is due to the following factors:

- Due to the lack of relevant support studies **the success criteria for a large non-isolatable break upstream of the MSIV are used for** dominant sequences of **a small steam line break** when the MSIVs are closed. This is a very conservative assumption. For example, RCP [RCS] boration is assumed to be required in the event of failure of ASG [EFWS] isolation on the affected SG for all sizes of non-isolatable breaks. Boration would not be expected to be required for small breaks.

- The small non-isolatable break initiating event is much more frequent compared to the large non-isolatable break.

- A large break downstream of the MSIV is isolatable when compared to a small break upstream of the MSIV. Thus, this event is much less risk significant.

5.3.3. Dominant Accident Sequences Analysis

The following table lists the main accident sequences in the secondary breaks group. Each accident sequence corresponds to one or a group of MCSs. The main accident sequences described in the table below represent 92% of the group CDF.

Initiating event	***Brief description of the accident sequence***	***Frequency (per reactor per year)***
SLB_SO_AB	The MSIV are closed **and** the operator fails (human error or I&C failure) to terminate ASG [EFWS] to the affected SG to prevent over-cooling **and** all MHSI fails due to mechanical failure or I&C failure.	1.0E-8
SLB_LO_AB	Failure to close of four MSIVs **and** MHSI fails due to I&C failure	2.0E-9

All the dominant accident sequences have a similar structure. Following the break, there are two sequences which culminate in core damage, i.e.:

- One SG is not isolated from the break and the operator fails to prevent over cooling by the automatic feeding of the affected SG by the Emergency Feedwater System (ASG [EFWS]).

- At least two SGs are not isolated from the break, after which some MHSI pumps fail due to either intrinsic failures or I&C failures preventing their automatic start.

Consequently, the dominant failures are:

- Failure to close of the MSIV to prevent overcooling of the RCP [RCS].

- Failure of the operator to isolate ASG [EFWS]. This manual isolation is the only means of preventing overcooling of the affected SG for non-isolatable breaks.

- Failure of the MHSI which would provide RCP [RCS] boration.

5.3.4. Initiating Events Analysis

The following responses apply for each initiating event of the secondary break group:

- For each SG, the Main Feedwater system (ARE [MFWS]) and the Start-up and Shutdown System (AAD [SSS]) are completely isolated. Both the full load and low load lines are isolated on a “SG pressure < MIN2” signal. Hence a SG which is blowing down is automatically isolated from the ARE [MFWS] and the AAD [SSS].

- Feed from the ASG [EFWS] to the affected SGs must be manually terminated to prevent uncontrolled cooling of these SGs.

- The over-cooling due to the steam line break causes a contraction of the reactor coolant. This results in a fall in pressure in the RCP [RCS] and emptying of the pressuriser. Consequently, the Medium Head Safety Injection (MHSI) system starts automatically and injects a significant quantity of extra-borated coolant into the RCP [RCS]. Thus, in the event of steam line break, operation of the MHSI system has a significant positive impact on the boron concentration.

5.3.4.1. Small Steam Line Break (SLB SO)

5.3.4.1.1. Event Description

The assumed break is equivalent to a spurious opening of one Main Steam Relief Train (VDA [MSRT]) which remains fully open or a Main Steam Safety Valve (MSSS) stuck-open, upstream of the Main Steam Isolation Valves (MSIV) and outside the containment.

This break results in an initial increase of steam production, but the steam flow to the atmosphere is less than that from a guillotine break. The increased energy removal from the RCP [RCS] causes a reduction in coolant temperature and pressure and an insertion of positive reactivity due to the negative moderator coefficient.

An “SG pressure drop” signal or “low SG- pressure” signal actuates reactor trip, the closure of all MSIVs and the closure of all Main Feedwater (ARE [MFWS]) full-load lines. All these actions are automatic. After MSIV closure, at least the MSIV of the affected SG is closed, the over-cooling is stopped on 3 out of 4 SGs but the affected SG continues to empty. When the affected SG is drained, it is conservatively assumed that the Emergency Feedwater system (ASG [EFWS]) which starts automatically must be shut down, to arrest the over cooling.

When the over cooling is terminated, the secondary side Residual Heat Removal (RHR) function is provided by the three unaffected SGs and their VDA [MSRT] systems. After a few hours the primary side is sufficiently cooled to connect the Residual Heat Removal system (RIS-RA [RHR]), thus providing the long term cooling. Thus a safe shutdown state has been reached.

5.3.4.1.2. Functional Safety Requirements

This section identifies the safety functions that are challenged by the small steam line break event in an at-power state. The same success criteria as those for a large break inside the containment are conservatively applied.

- **Reactivity Control:** Reactivity control is provided by the reactor trip. It is conservatively assumed that an automatic and a manual isolation of SG feed are also required. Consequently, the operator has to shut off the ASG [EFWS] train on the affected SG. The failure probability of the automatic ARE [MFWS]/AAD [SSSS] Low Load line isolation is negligible when compared with that of the manual isolation of ASG [EFWS]. Therefore it has not been considered in the analysis.

  The consequences of rod drop failure following failure to close the MSIV of the affected SG are not considered in this section. The reactor trip failure is assessed in section 5.10 of this sub-chapter covering Anticipated Transients Without Scram. If more than one MSIV fails to close core damage is assumed to occur.

If the operator fails to shut down the ASG [EFWS] trains, boration of the RCP [RCS] is required and is achieved by the MHSI automatically actuated on a low RCP [RCS] pressure.

If several MSIVs including those on the affected SG fail to close, the reactor trip and the operator actions are insufficient to provide reactivity control. Whatever the operator actions are, boration of the primary circuit is required by the MHSI.

Accumulator actuation is claimed only when four SGs are blown down because it is conservatively assumed that their injection pressure is not reached in other cases.

The Extra Boration System (RBS [EBS]) is conservatively not claimed. Firstly, the scope and design of the automatic actuation of RBS [EBS] on low Steam Generator pressure in one Steam Generator are at an early stage and remain to be fully defined. Secondly, for reasons of simplification, manual initiation of the Extra Boration System (RBS [EBS]) is also conservatively not claimed, even if the Emergency Operating Procedures require it.

- Remove core decay heat and stored heat. This safety function is divided into:

  - **Residual Heat Removal**: Once the over cooling is halted, the RHR function is provided by the unaffected SGs. They are fed by the Main Feedwater System (ARE [EFWS]) or by the Startup and Shutdown System (AAD [SSS]), started automatically following a “ARE [MFWS] pumps off” signal. Steam is released to the atmosphere via the VDA [MSRT] control valves.

    Should failure of the ARE [MFWS] and AAD [SSS] systems occur, the ASG [EFWS] system starts automatically when the “low low SG level” setpoint is reached.

    If the over cooling is not controlled, all SGs remain connected to the break, the RIS-RA [RHR] connection conditions are still achieved as long as sufficient shutdown margin is provided by reactor trip and RCP [RCS] boration.

    Should failure of the secondary side RHR occur, primary side RHR via Feed & Bleed is initiated by the operator. The Primary Depressurisation Valves or the Pressuriser Safety Valves are opened, and the safety injection system is started.

  - **Long term cooling:** Long term cooling is provided by the RIS-RA [RHR] system.

- **Reactor Coolant System integrity:** The RCP [RCS] integrity is challenged in the case of Feed and Bleed operation.

- **Reactor Coolant System inventory control:** The over-cooling causes a contraction of the primary coolant and, consequently, an RCP [RCS] depressurisation but this contraction does not lead to core uncovery. The RCP [RCS] inventory control function is only challenged in the event of feed and bleed. In that case it is met by the MHSI.

5.3.4.1.3. Detailed Results

The “small steam line break” (upstream of MSIV) represents **2% of the Internal Event CDF, with a frequency of 1.1E-8/r.y.**

The following table lists the main accident sequences. Each accident sequence corresponds to one or a group of MCSs. The main accident sequences considered in the table below represent 96% of the initiating event risk.

Initiating event	***Brief description of the accident sequence***	***Frequency (per reactor per year)***
SLB_SO_AB	The MSIV are closed **and** the operators fail (human error or I&C failure) to shut down the ASG [EFWS] to the affected SG to terminate the over cooling **and** all MHSI fails due to mechanical failure or I&C failure.	1.0E-8
SLB_SO_AB	There is more than one affected SG due to the failures to close of the MSIV **and** MHSI fails	4.4E-10

The following systems are important in the protection against “small steam line break upstream of an MSIV”:

- The **MSIVs** are very important because their closure significantly reduces the overcooling.
- **MHSI** is important because it provides the RCP [RCS] boration and thus contributes to reactivity control. The MHSI is not as important for RCP [RCS] inventory control as in many other fault groups.
- **Reactor trip** is important because reactivity control is the most significant safety concern following a steam line break.

The following operator action is important in the protection against “small steam line breaks upstream of MSIV”:

- **Isolation of ASG [EFWS] train(s) in the affected SG(s)** is important because it is the only back-up to MHSI failure.

The following I&C signals and systems are important in the protection against “small line break upstream of an MSIV”:

- SPPA-T2000 platform is required in MHSI start up (diversified signal) and manual isolation of ASG [EFWS].

5.3.4.2. Large Steam Line Break Downstream of MSIV (SLB LO)

5.3.4.2.1. Event Description

The break considered is a guillotine break on the main steam line downstream of the Main Steam Isolation Valve (MSIV).

The main differences between this and the small break are:

- Steam flow is higher. Thus, the signal “SG pressure drop” or “low SG- pressure” signal is generated earlier than it would be following a small break.

- After the MSIV closure, over cooling is terminated on all SGs as no SG is connected to the break.

Consequently following the automatic MSIV closure, the Residual Heat Removal is provided by 4 SGs and there is no isolation of ARE/AAD feed to the SGs. After a few hours the primary side is sufficiently cooled to allow connection of the Residual Heat Removal system (RIS-RA [RHR]). Thus provides the long term cooling and a safe shutdown state has been reached.

5.3.4.2.2. Functional Safety Requirements

The safety functions are the same as those identified for a small steam line break (see section 5.3.4.1.2 above). If all MSIV close, then a reactor trip is sufficient to control the reactivity.

5.3.4.2.3. Detailed Results

The “large steam line break” (downstream of the MSIV) represents **0.4% of the Internal Event CDF, with a frequency of 2.1E-9/r.y.**

The following table lists the main accident sequences. Each accident sequence corresponds to one or a group of MCSs. The main accident sequence considered in the table below represents 97% of the initiating event risk.

Initiating event	***Brief description of the accident sequence***	***Frequency (per reactor per year)***
SLB_LO_AB	The MSIV fail to close **and** all MHSI fails due to I&C failure	2.0E-9

The following systems are important in the protection against “large steam line break downstream of an MSIV”:

- The **MSIVs** are important because their closure significantly reduces the overcooling.

- **MHSI** is important because it provides the RCP [RCS] boration and thus contributes to reactivity control. The MHSI is not as important for RCP [RCS] inventory control as in many other fault groups.

The following I&C signals/systems are important in the protection against “large steam line break downstream of an MSIV”:

- **TXS** platform is required for MSIV closure and MHSI start up.

- **SPPA-T2000** platform for required in MSIV closure and MHSI start up.

5.3.4.3. Large Steam Line Break Inside Containment (SLB LI)

5.3.4.3.1. Event Description

The break considered is a guillotine break of a main steam line **inside** the containment.

The main difference between this and a break outside the containment is that, after closure of the MSIVs, at least the closure of the MSIV on the affected SG, over-cooling is terminated on 3 out of 4 SGs with the affected SG blowing down.

Consequently, when the affected SG is blown down, the Emergency Feedwater System (ASG [EFWS]), which starts automatically, must be shut down to halt the over-cooling.

5.3.4.3.2. Discussion

The main differences between the large steam line break inside the containment (SLB_LI_AB) and the small steam line break upstream of an MSIV (SLB_SO_AB) are:

- The overcooling is greater because the affected SG blows down more rapidly.
- If at least two SGs blow down inside the containment there will be a pressure transient in the containment. This pressure transient will not lead to containment rupture.

The fact that the event SLB_LI_AB is not dominant compared to the event SLB_SO_AB can be explained by the fact that the frequency of the initiating event SLB_LI_AB is much lower than that of the SLB_SO_AB and because they share the same dominant sequence when all MSIVs are closed.

5.4. STEAM GENERATOR TUBE RUPTURE (SGTR)

5.4.1. Group Description

The initiating event considered is a Steam Generator Tube Rupture, one tube rupture and two tubes ruptured, when the reactor is initially at full power operation (state A) and in shut down with secondary-side heat removal (state B).

Steam Generator Tube Rupture (SGTR) causes a loss of coolant inventory from the primary to the secondary side of the affected SG. The leak rate for one tube rupture is around 20 kg/s, the initial value for the full power state, and leads to a primary pressure decrease and a level increase in the affected SG.

The mitigation objective, after reactor trip, is to stop the leak by equalising the primary and secondary pressures. The principal requirement is the isolation of the affected SG to limit the release outside the containment. This requires actions to limit the filling of the affected SG, and in particular, to avoid the steam valves opening under water relief. The setpoint of the Main Steam Relief Valves (VDA [MSRV]) is automatically modified to limit the possibility of their actuation.

The transient is terminated when the affected SG is isolated and the main primary parameters are controlled.

For the case of one tube rupture, the Chemical and Volume Control System (RCV [CVCS]) is able to match the loss of reactor coolant inventory. Reactor Trip (RT) will occur when a “SG level > MAX1” signal is generated. Partial cooldown is then automatically initiated following a “SG level > MAX2” signal. At the end of the partial cooldown, the affected SG is isolated, and the (RCV [CVCS]) is shutdown. Reactor trip can also be actuated on a “pressuriser (PZR) pressure < MIN2” signal which occurs about 30 minutes after the start of the transient. If the volume control system is in service the Safety Injection System (RIS [SIS]) will not be actuated.

For the case of rupture of two tubes, the Safety Injection System (RIS [SIS]) is required to compensate for the loss of reactor coolant inventory. RT will be actuated following either a “PZR pressure < MIN2” or “SG level > MAX1” signal. The Safety Injection System (RIS [SIS]) will be actuated following a “PZR pressure <MIN3” signal. Partial cool-down will be initiated following a Safety Injection (SI) signal or “SG level > MAX2” signal. At the end of the partial cooldown the affected SG is isolated and the Chemical and Volume Control System (RCV [CVCS]) is shutdown.

For sequences in which isolation fails, but a safe state is reached before the In-containment Refuelling Water Storage Tank (IRWST) empties, core damage can be prevented.

The following initiating events are considered in the group:

- Steam generator tube rupture (1 tube) in state A and B: SGTR1_AB
- Steam generator tube rupture (2 tubes) in state A and B: SGTR2_AB

The definitions and frequencies of the initiating events are given in section 4 of this sub-chapter.

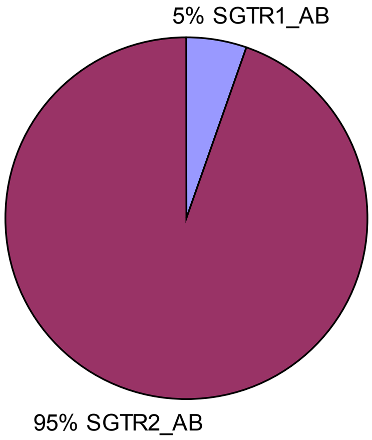
5.4.2. Results

The contribution of Steam Generator Tube Ruptures to the internal events **Core Damage Frequency is 4.2E-9/r.y**, which represents **0.8% of the internal event CDF.**

The CDF for each SGTR initiating event within the group is shown in the following table:

Initiating Event	IE frequency (/y)	CDF(/r.y)
SGTR1_AB	{CCI} [a]	2.2 E-10
SGTR2_AB	{CCI} [a]	4.0 E-9
total		4.2 E-9

The relative contribution of each SGTR initiating event within the group is given below:



The low contribution of SGTR transients to the CDF is due to the robust design of the EPR. In particular release is limited by the effective control of the level in the affected SG as a result of the following measures:

- The MHSI pumps have a low pressure head which avoids the actuation of the secondary steam valves.

- The RCV [CVCS] pumps are automatically tripped when the affected SG level is high.

5.4.3. Dominant Accident Sequences Analysis

The following table lists the main accident sequences in the steam generator tube rupture group. The main accident sequences presented in the table below represent 98% of the overall group risk.

Initiating event	***Brief description of the accident sequence***	***Frequency per reactor per year***
SGTR2_AB	MHSI trains fail either due to intrinsic failure or due to I&C failure **and** fast secondary cooldown fails either due to operator failure or due to I&C failure.	3.9E-9
SGTR1_AB	RCV [CVCS] pumps are not available **and** MHSI trains fail **and finally** fast secondary cooldown fails.	1.5E-10
SGTR1_AB	Partial cooldown fails **and** the operator fails to manually isolate the RCV [CVCS] before the SG overfills **and** fast secondary cooldown fails **and finally** feed and bleed fails.	2.2E-11
SGTR2_AB	Partial cooldown fails **and** the operator fails to manually isolate the RCV [CVCS] before the SG overfills **and finally** the operator fails to initiate the cooling before the IRWST empties.	1.1E-11
SGTR1_AB	Automatic RCV [CVCS] isolation fails **and** the operator fails to manually isolate the RCV [CVCS] before the SG overfills **and finally** the operator fails to initiate the cooling before the IRWST empties.	1.1E-11
SGTR2_AB	Automatic RCV [CVCS] isolation fails **and** the operator fails to manually isolate the RCV [CVCS] before the SG overfills **and finally** the operator fails to initiate the cooling before the IRWST empties.	9.0E-12

The dominant sequences are divided into 3 types of scenarios:

- The failure of cooldown (partial or fast) which is necessary for the equalisation of the primary and the secondary pressure and hence stop the leak.

- The affected SG isolation fails which results in a secondary break and then containment by pass. In this case, if the primary to secondary leak is not terminated before the IRWST empties, the reactor coolant inventory is not controlled. Failure to isolate the affected SG can be due to RCV [CVCS] isolation failure which will fill the SG with a risk of SG relief valves opening and no re-closure. It can also result from a failure to isolate the SG on the inlet or outlet side.

- There is no water supply to compensate for the leak due to the SGTR because the Medium Head Safety Injection (MHSI) for SGTR2_AB, and the RCV [CVCS] pumps and MHSI trains for SGTR1_AB, are unavailable. It is then, necessary, for the operator to cooldown as fast as possible to conserve water inventory. In the event of failure of this fast secondary cooldown, there is a risk of core damage.

5.4.4. Initiating Events Analysis

5.4.4.1. Steam Generator Tube Rupture (1 tube) (SGTR 1T)

5.4.4.1.1. Event Description

The initiating event of Steam Generator Tube Rupture (1 tube) corresponds to a rupture with a leak of 20kg/s, the initial value during the full power state, which can be matched by the RCV [CVCS].

The inventory of the Reactor Coolant System (RCP [RCS]) decreases and the level in the affected SG increases following the rupture of one tube. Due to the decrease of RCP [RCS] inventory the PZR level drops and the second RCV [CVCS] pump is started. The affected SG fills to the MAX1 level. The resultant “SG level > MAX1” signal results in reactor trip and the Main Feed Water System (ARE [MFWS]) is isolated. When the “SG Level > MAX2” setpoint is reached a partial cooldown is actuated. At the end of the partial cooldown, the affected SG is isolated either automatically or manually. Isolation is performed on the steam side by closing the Main Steam Isolation Valve (MSIV) and by increasing the set point of the Main Steam Relief Valves (VDA [MSRV]) to a value above the MHSI discharge pressure. The RCV [CVCS] is also automatically isolated at the end of partial cooldown. This isolation is necessary to avoid the SG filling and the risk of containment bypass. The short term phase ends with the isolation of the SG and the RCV [CVCS].

5.4.4.1.2. Functional Safety Requirement

This sub-chapter presents the safety functions which are challenged by a Steam Generator tube rupture (1 tube).

- **Reactivity Control**: Reactivity control is provided by reactor trip. The consequences of a failure of reactor trip are not considered in this section. They are considered in section 5.10 of this sub-chapter on Anticipated Transients Without Scram.

  During the cooling of the plant, there is a risk of backflow from the secondary side to the primary side with the potential formation of a cold unborated water plug if the primary pumps are tripped. To avoid this scenario which could affect reactivity, the post accident operating procedures require a reduction in pressure in the affected SG to control the rate of fall of primary pressure. This scenario is very unlikely and has been neglected.

- Removal of core decay heat and stored heat. This safety function is divided into:

  - **Residual Heat Removal**: this function is not affected by this transient. It is only required if the affected SG is not isolated to enable the primary circuit to cool down as quickly as possible to atmospheric pressure and a temperature below 100°C terminate the leak. All the usual RHR systems can be used to reach this safe state (secondary RHR, RIS-RA [RHR] and feed and bleed if necessary).

  - **Long term cooling**: this function is not affected by this transient.

- **Reactor Coolant System integrity**: The initiating event breaches the RCP [RCS].

- **Reactor Coolant System inventory control**: RCP [RCS] inventory control is performed by

  - The RCV [CVCS] or the RIS [SIS] if the RCV [CVCS] is not available,

  - Limitation of the primary to secondary pressure differential.

  - Isolation of the affected SG.

    The RCP [RCS] inventory is challenged in the event of SG isolation failure. In this case, it is necessary to cooldown very rapidly to 100°C and a pressure of 1 bar

5.4.4.1.3. Detailed Results

The "Steam Generator Tube Rupture (1 tube)" represents **0.04% of the internal event CDF with a frequency of 2.2E-10/r.y**.

The following table lists the main accident sequences. Each accidental sequence corresponds to one or a group of MCS. The main accident sequences considered in the table below represent 91% of the initiating event risk.

Initiating event	***Brief description of the accident sequence***	***Frequency per reactor per year***
SGTR1_AB	RCV[CVCS] pumps are not available **and** MHSI trains fail **and finally** fast cooldown fails.	1.5E-10
SGTR1_AB	Partial cooldown fails **and** the operator fails to manually isolate the RCV [CVCS] before the SG overfills **and** fast secondary cooldown fails **and finally** feed and bleed fails.	2.2E-11
SGTR1_AB	Automatic isolation of RCV [CVCS] fails after partial cool-down **and** the operator fails to manually isolate the RCV [CVCS] before the SG overfills **and finally** the operator fails to initiate the cooling before the IRWST empties.	1.1E-11
SGTR1_AB	SG isolation fails **and** the operator fails to initiate the cooling before the IRWST empties.	8.8E-12
SGTR1_AB	MAX2 on affected SG fails **and** the operator fails to manually isolate the RCV [CVCS] before SG overfills **and finally** the operator fails to initiate the cooling before the IRWST empties.	7.6E-12

The following systems are important to the protection against “Steam Generator tube rupture (1 tube)”:

- Systems involved in secondary cooldown, **AAD/ASG [SSS/EFWS] and GCT [MSB] / VDA [MSRT]** are important because they provide the RCP [RCS] inventory control.

- Systems involved in **feed and bleed** are important because they provide the RCP [RCS] inventory control.

- **RCV [CVCS]** and **MHSI** for make up in case of SGTR are important because they provide the RCP [RCS] inventory control.

- Automatic isolation of **RCV [CVCS]** for “SG level > MAX2” after partial cooldown is important because it provides RCP [RCS] inventory control.

- **Isolation of the affected SG** by set point increase is important because it provides RCP [RCS] inventory control.

The following operator actions are important in the protection against “Steam Generator tube rupture (1 tube)”:

- The operator recovery action **“manual RCV [CVCS] isolation”** is important because it limits the risk of SG overfilling and provides the RCP [RCS] inventory control, in the event of failure of automatic isolation.

- The action **“initiation of the cool-down before IRWST empties”** is important because it provides the RCP [RCS] inventory control in the event of failure of automatic actions.

The following I&C signals and systems are important in the protection against “Steam Generator tube rupture (1 tube)”:

- **SPPA-T2000**. This platform is required to initiate the manual cooldown and to start up the MHSI (diversified signal).

5.4.4.2. Steam Generator Tube Rupture (2 tubes) (SGTR 2T)

5.4.4.2.1. Event Description

The initiating event Steam Generator Tube Rupture (2 tubes) actuates the Safety Injection signal and leads to the automatic start of the MHSI.

The inventory of the Reactor Coolant System (RCP [RCS]) decreases and the SG level in the affected SG increases following a SG tube rupture. Due to the SGTR leak, the PZR pressure drops and the affected SG level increases. Reactor trip is actuated following a "PZR pressure < MIN2" or "SG level > MAX1" signal. The Main Feed Water System (ARE [MFWS]) is isolated following a "SG level > MAX1" signal. RIS [SIS] is started following a "PZR pressure < MIN3" signal and a partial cooldown is initiated. At the end of the partial cooldown, the affected SG is isolated either automatically or manually. Isolation is performed on the steam side by closing the Main Steam Isolation Valve (MSIV) and by increasing the setpoint of the Main Steam Relief Valve (VDA [MSRV]) to a value above the MHSI discharge pressure. The RCV [CVCS] is also isolated at the end of the partial cooldown. This isolation is required to prevent the SG filling and the risk of containment bypass. The short phase ends with the isolation of the SG and the RCV [CVCS].

5.4.4.2.2. Functional Safety Requirements

- **Reactivity Control**: Reactivity control is provided by the reactor trip. The consequences of a failure of reactor trip are not considered in this section. They are considered in section 5.10 of this sub-chapter on Anticipated Transient Without Scram.

  During the cooling of the plant, there is a risk of backflow from the secondary side to the primary side leading to the potential formation of a cold and unborated water plug if the primary pumps are tripped. To avoid this scenario which could affect reactivity, the post accident operating procedures require a reduction in pressure in the affected SG to control the rate of fall of primary pressure. This scenario is very unlikely and has been neglected.

- Removal of core decay heat and stored heat. This safety function is divided into:

  - **Residual Heat Removal**: this function is not affected by this transient. It is required if the affected SG is not isolated to enable the primary circuit to cooldown as quickly as possible to atmospheric pressure and a temperature below 100°C to terminate the leak. All the usual RHR systems can be used to arrive at this safe state (secondary RHR, RIS-RA [RHR] and feed and bleed if necessary).

  - **Long term cooling**: this function is not affected by this transient

- **Reactor Coolant System Integrity**: The initiating event breaches the RCP [RCS].

- **Reactor Coolant System Inventory**: The RCP [RCS] inventory control is performed by

  - RIS [SIS],

  - Limitation of the primary to secondary pressure control differential,

  - Isolation of the affected SG.

The RCP [RCS] inventory is challenged in the event of SG isolation failure. In this case, it is necessary to cooldown to 100°C and 1 bar pressure very rapidly.

5.4.4.2.3. Detailed Results

The “Steam Generator Tubes Rupture (2 tubes)” represents **0.75% of the internal event CDF with a frequency of 4.0E-9/r.y**.

Dominant cutsets:

The following table lists the main accident sequences. Each accident sequence corresponds to one or a group of MCSs. The main accident sequences considered in the table below represent 99% of the initiating event risk.

Initiating event	***Brief description of the accident sequence***	***Frequency per reactor per year***
SGTR2_AB	MHSI trains fail either due to intrinsic failure or due to I&C failure **and** fast secondary cooldown fails either due to operator failure or due to I&C failure..	3.9E-9
SGTR2_AB	Partial cooldown fails **and** the operator fails to manually isolate the RCV [CVCS] **and finally** the operator fails to initiate the cooling before the IRWST empties.	1.1E-11
SGTR2_AB	Automatic RCV [CVCS] isolation after partial cooldown fails **and** the operator fails to manually isolate the RCV [CVCS] before the SG overfills **and finally** the operator fails to initiate the cooling before IRWST empties.	9.0E-12
SGTR2_AB	Partial cooldown fails **and** the operator fails to manually isolate the RCV [CVCS] before the SG overfills **and** fast cooldown fails **and finally** feed and bleed fails.	7.4E-12

The following systems are important in the protection against “Steam Generator tubes rupture (2 tubes)”:

- Systems involved in secondary cooldown, **AAD/ASG [SSS/EFWS] and GCT [MSB] /VDA [MSRT]** are important because they provide the RCP [RCS] inventory control.
- **MHSI** trains are important because they provide RCP [RCS] inventory control.
- Automatic isolation of **[RCV] CVCS** on “SG level > MAX2” after partial cooldown is important because it provides RCP [RCS] inventory control.

The following operator actions are important in the protection against “Steam Generator tube rupture (2 tubes)”:

- The action **“initiation of the cool-down before IRWST empties**” is important because it provides the RCP [RCS] inventory control in the event of failure of automatic actions.

The following I&C signals and systems are important in the protection against “Steam Generator tube rupture (2 tubes)”:

- **SPPA-T2000**. This platform is required to initiate the manual cooldown and to start up MHSI (diversified signal)

Note: The operator recovery action “**manual RCV [CVCS] isolation”** is not claimed because of the short time to SG filling.

5.5. INDUCED STEAM GENERATOR TUBE RUPTURE

5.5.1. Group Description

The initiating event considered is a Steam Generator Tube Rupture (SGTR) induced by a Steam Line Break (SLB) when the reactor is initially at full power operation (state A) and shutdown with secondary side heat removal (state B).

The Steam Generator (SG) pressure decreases following the SLB. The increased pressure differential between the primary and secondary can cause a SGTR in the SG affected by the SLB. The resultant SGTR is assumed to be equivalent to 2 tubes. The consequences of this accident are a fast and uncontrolled cooldown of the Reactor Coolant System (RCP [RCS]) which can cause an increase of reactivity. MHSI is needed for reactivity control and reactor coolant inventory control.

The following initiating events are considered, consistent with those considered for the SLB group:

- Induced steam generator tube rupture following a large break inside the containment in state A and B: SLB LI SGTR_AB

- Induced steam generator tube ruptures following a large break outside the containment and downstream of the MSIV in state A and B: SLB LO SGTR_AB.

- Induced steam generator tube rupture following a small break outside the containment and upstream of the MSIV in state A and B: SLB SO SGTR_AB

The definition and frequencies of the initiating events are given in section 4 of this sub-chapter.

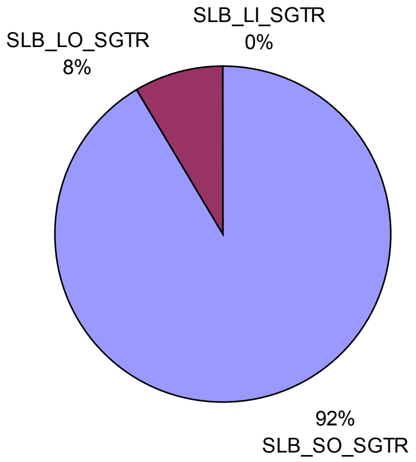
5.5.2. Results

The contribution of the induced steam Generator tube ruptures group to the internal events **Core Damage Frequency is 4.3E-09/r.y** which represents **0.8% of the internal event CDF.**

The CDF for each induced SGTR initiating event within the group is shown in the following table:

Initiating Event	IE frequency (/y)	CDF(/r.y)
SLB LI SGTR_AB	{CCI} [a]	5.2E-12
SLB LO SGTR_AB	{CCI} [a]	3.7E-10
SLB SO SGTR_AB	{CCI} [a]	3.9E-9
total		**4.3E-09**

The relative contribution of each induced SGTR initiating event within the group is given below.



The group risk is dominated by the induced SGTR after a small steam line break upstream of the MSIV (SLB SO SGTR_AB). This analysis is consistent with the SLB group analysis and with the fact that the SGTR cannot be isolated because of the location of the break.

5.5.3. Dominant Accident Sequences Analysis

The following table lists the main accident sequences of the induced steam generator tube rupture group. The main accident sequences considered in the table below represent more than 99% of the overall group risk.

Initiating event	***Brief description of the accident sequence***	***Frequency per reactor per year***
SLB_SO_SGTR_AB	An SGTR induced by a small break upstream of the MSIV **and** the MHSI trains are unavailable.	3.6E-9
SLB_LO_SGTR_AB	An SGTR induced by a large break downstream of the MSIV **and** the MSIV on the affected SG fails to close **and finally** a further MSIV fails to close.	3.6E-10
SLB_SO_SGTR_AB	An SGTR induced by a small break upstream of the MSIV **and** the operator fails to cool down before the IRWST empties.	2.0E-10
SLB_SO_SGTR_AB	An SGTR induced by a small break upstream of the MSIV **and** the LHSI trains are unavailable for RHR.	1.2E-10

SGTR following a small break upstream of the MSIV represents 92% of the overall risk group.

The main risk significant events after a small break are:

- MHSI is unavailable with a consequent loss of reactor coolant inventory due to the SGTR and a loss of reactivity control due to the SLB.
- LHSI used in RHR mode is unavailable or the operator fails to initiate the cool down to terminate the primary to secondary leak before the IRWST empties. This would challenge the reactor coolant inventory control.

5.5.4. Initiating Event Analysis

5.5.4.1. Small Steam line break upstream of the MSIV and induced SGTR (SLB_SO_SGTR_AB)

5.5.4.1.1. Event description

The initiating event “Small SLB upstream of MSIV and induced SGTR” corresponds to a non isolated SGTR of 2 tubes. In this analysis the MSIVs are conservatively assumed to remain open. The start up of the MHSI is required to control the reactivity.

The Reactor Coolant System (RCP [RCS]) temperature decreases following the SLB. At the same time the RCP [RCS] coolant inventory decreases due to the SGTR. Reactor trip is actuated on the SLB parameters “SG pressure drop” and “low-SG pressure”. The MHSI is needed for reactor coolant inventory control.

5.5.4.1.2. Functional Safety Requirements

- **Reactivity Control**: Reactivity control is provided by reactor trip. To be conservative, the MSIVs are assumed to be open and the MHSI is required for reactivity control. The consequences of a failure of the reactor trip are not considered in this section. They are considered in section 5.10 of this sub-chapter on Anticipated Transients Without Scram. The consequence of an unavailability of the MHSI is core damage.
- Removal of core decay heat and stored heat: This safety function is divided into:
    - **Residual Heat Removal**: It is necessary to get down to atmospheric pressure with the temperature below 100°C as soon as possible to terminate the leak. All the normal RHR systems can be used to reach this safe state (RIS-RA [RHR] and feed and bleed if necessary).
    - **Long term cooling**: This function is not considered in this section.
- **Reactor Coolant System Integrity**: the reactor coolant system is breached by the initiating event.
- **Reactor Coolant System Inventory**: RCP [RCS] inventory control is achieved by
    - The Safety Injection System RIS [SIS],
    - The cool down of the RCP [RCS] below 100°C/1 bar to terminate the SGTR leak.

5.5.4.1.3. Detailed Results

The “Small SLB upstream of MSIV and induced SGTR” represents **0.7% of the internal event CDF with a frequency of 3.9E-9/r.y**.

The following table lists the main accident sequences. Each accident sequence corresponds to one or a group of MCSs. The main accident sequences considered in the table below represent 99% of the initiating event risk.

Initiating event	***Brief description of the accident sequence***	***Frequency per reactor per year***
SLB_SO_SGTR_AB	An SGTR induced by a small break upstream of the MSIV **and** the MHSI trains are unavailable.	3.6E-9
SLB_SO_SGTR_AB	An SGTR induced by a small break upstream of the MSIV **and** the operator fails to cooldown before the IRWST empties.	2.0E-10
SLB_SO_SGTR_AB	An SGTR induced by a small break upstream of the MSIV **and** the LHSI trains are unavailable for RHR.	1.2E-10

The following system is important in the protection against “Small SLB upstream of the MSIV and induced SGTR”

- **MHSI** availability is important because it provides the RCP [RCS] inventory and reactivity control.
- **LHSI** used in RHR mode availability is important because it provides cooling of the RCP [RCS] to primary conditions which terminates SGTR leak and thereby provides the RCP [RCS] inventory control.

The following operator action is important in the protection against “Small SLB upstream of the MSIV and induced SGTR”:

- The action **“initiation of the cool down before IRWST empties”** is important because it provides the RCP [RCS] inventory control.

5.5.4.2. Large Steam Line Break downstream of the MSIV and induced SGTR (SLB_LO_SGTR_AB)

5.5.4.2.1. Event description

The break considered is a guillotine break of a main steam line downstream of the MSIV.

The main differences to the small break are:

- Steam flow is greater. Thus an “SG pressure drop” or “low SG-pressure” signal is produced earlier than in case of small break.

- Following MSIV closure, the overcooling is halted on all the SGs. The transient is then the same as SGTR - 2 tubes.

In the event of failure to close of the MSIV on the affected SG, the SGTR is not isolated. In this case it is necessary to cool down as quickly as possible to terminate the leak.

It is conservatively assumed in this analysis that the failure to close of 2 MSIV, the MSIV on the affected SG and one other, leads to core damage.

5.5.4.2.2. Functional Safety Requirements

- **Reactivity Control**: Reactivity control is provided by reactor trip and by the MHSI when needed. The consequences of failure of reactor trip are not considered in this section. They are considered in section 5.10 of this sub-chapter on Anticipated Transients Without Scram. The consequence of the unavailability of the MHSI is core damage.

- Removal of core decay heat and stored heat. This safety function is divided into:

  - **Residual Heat Removal**: It is necessary to reach atmospheric pressure and a temperature below 100°C as soon as possible to terminate the leak. All the usual RHR systems can be used to reach this safe state (RIS-RA [RHR] and feed and bleed if necessary).

  - **Long term cooling**: This function is not considered in this section.

- **Reactor Coolant System Integrity**: the primary coolant boundary is breached by the initiating event.

- **Reactor Coolant System Inventory**: RCP [RCS] inventory control is performed by:

  - The Safety Injection System RIS [SIS],

  - Cool down of the RCP [RCS] to 100°C/1 bar which is necessary to terminate the SGTR leak

5.5.4.2.3. Detailed Results

The “Large Steam Line Break downstream MSIV and induced SGTR” represents **0.07% of the internal event CDF, with a frequency of 3.7 E-10/r.y**.

The following table lists the main accident sequence. The accident sequence corresponds to one or a group of MCSs. The main accident sequence considered in the table below represents 99% of the initiating event risk.

Initiating event	*Brief description of the accident sequence*	*Frequency per reactor per year*
SLB_LO_SGTR_AB	An SGTR induced by a large break downstream of the MSIV **and** failure to close of the MSIV on the affected SG **and finally** a further MSIV fails to close.	3.6E-10

The following systems are important in the protection against “Large Steam Line Break downstream of the MSIV and induced SGTR”:

- **MSIV** closure on the SG affected by the SGTR is important because it provides Reactor Coolant System inventory control. **MSIV** closure on the other SGs is important for reactivity control. This is a conservative assumption.

5.5.4.3. Large Steam Line Break inside containment and induced SGTR (SLB_LI_SGTR_AB)

5.5.4.3.1. Event description

The break considered is a guillotine break on the main steam line inside containment (upstream of the Main Steam Isolation Valves (MSIV)) followed by an SGTR.

The Reactor Coolant System (RCP [RCS]) temperature decreases following the SLB. At the same time the RCP [RCS] coolant inventory decreases due to the SGTR. The reactor trip will be actuated following a “SG pressure drop” or “Low SG pressure” Signal.

In this analysis, the failure to close of 2 MSIV is assumed to lead to core damage.

5.5.4.3.2. General considerations

For SGTR induced by a large break inside the containment and one SG blow down in containment, the core damage frequency is insignificant.

If at least two SG blow down in the containment, in addition of core damage, there is a pressure transient in the containment. This pressure transient will not lead to containment rupture.

This initiating event is not developed due to the low frequency of the scenario.

5.6. SECONDARY TRANSIENTS

5.6.1. Group Description

The Secondary Transients group deals with initiating events that cause steam generator feedwater perturbations during normal operation. The transients are studied during at-power states (state A) and in intermediate shutdown (state B).

These transients create a sudden and significant imbalance between the thermal power produced by the primary side and the capacity of power extraction by the secondary side. The mitigation terminates the power production by a reactor trip and re-establishes secondary cool-down using the available systems. The turbine is tripped and the residual power is removed either by the Main Steam Bypass (GCT [MSB]) or by the Main Steam Relief Train (VDA [MSRT]).

Following reactor trip, the low load line of the Main Feedwater System (ARE) [MFWS] or the Start-up and Shutdown System (AAD [SSS]) are actuated to feed the steam generators. If these systems are unavailable, the Emergency Feedwater System (ASG [EFWS]) starts automatically.

After a few hours the primary side is sufficiently cooled to connect the Residual Heat Removal system (RIS-RA [RHR]) which provides long term cooling. The safe shutdown state is then reached.

The following initiating events are considered in the group:

- Total loss of ARE [MFWS] during at-power state A (LOMFW_A),
- Total loss of AAD [SSS] during intermediate shutdown B (LOSSS_B).
- Spurious Turbine Trip during at-power state A (TT_A),
- Loss of the condenser during at-power states A and B (LOC_AB),

The definition and frequencies of the initiating events are described in section 4 of this sub-chapter. The frequencies are tabulated in the following section.

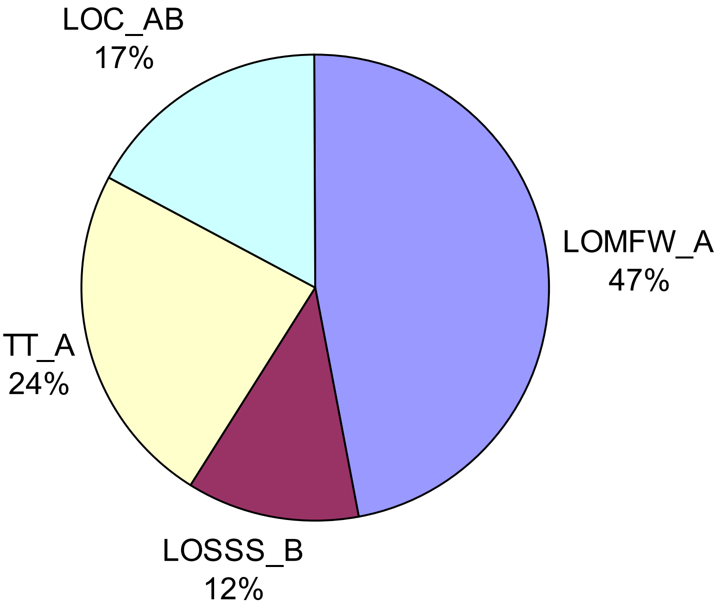
5.6.2. Results

The contribution of the secondary transients group to the **Internal Event Core Damage Frequency is 1.8E-08/r.y** which represents **3.4% of the Internal Event CDF**.

The CDF for each secondary transient initiating event within the group is shown in the following table:

Initiating Event	IE frequency (/y)	CDF (/r.y)
LOMFW_A	{CCI}[a]	8.41E-09
LOSSS_B	{CCI}[a]	2.16E-09
TT_A	{CCI}[a]	4.28E-09
LOC_AB	1.50E-01	3.09E-09
total		1.79E-08

The relative contribution of each secondary transient initiating event within the group is given below:



5.6.3. Dominant Accident Sequences Analysis

The following table lists the main accident sequences in the secondary transients group. Each accident sequence corresponds to one or a group of Minimal Cutsets (MCSs). The main accident sequences considered in the table below represent 93% of the overall group CDF.

Initiating event	***Brief description of the accident sequence***	***Frequency (per reactor per year)***
LOMFW_A	The AAD [SSS] system fails **then** the ASG [EFWS] fails due to a CCF (or CCF with preventive maintenance) **and finally** the operators do not initiate primary bleed	4.6E-09
TT_A	ARE [MFWS] and AAD [SSS] fail due to total loss of digital I&C **and** the operator fails to manually start and control the ASG [EFWS] **and finally** the operator fails to initiate the primary Feed and Bleed or to initiate IRWST cooling with EVU [CHRS]	4.1E-09
LOC_AB	ARE [MFWS] and AAD [SSS] fail due to total loss of digital I&C **and** the operator fails to manually start and control the ASG [EFWS] **and finally** the operator fails to initiate the primary Feed and Bleed or to initiate IRWST cooling with EVU [CHRS]	2.3E-09
LOMFW_A	Total digital I&C failure causes the loss of the VDA [MSRT] and AAD [SSS] systems **then** operator fails to manually start or control the ASG [EFWS] **and finally** the primary Feed and Bleed fails	1.8E-09

Initiating event	*Brief description of the accident sequence*	*Frequency (per reactor per year)*
LOSSS_B	The ASG [EFWS] fails to start due to an I&C failure **and** the operator fails to manually start ASG [EFWS] and to start ARE [MFWS] **and finally** the operators do not initiate primary bleed or IRWST cooling	1.7E-09
LOMFW_A	The AAD [SSS] system fails **then** the ASG [EFWS] fails due to an I&C failure and the operator fails to manually start or control the ASG [EFWS] **and finally** the operators do not initiate primary bleed	9.3E-10
LOC_AB	An I&C failure causes the failure of VDA [MSRT] valves **then** the operator does not initiate make-up to the tanks **and finally** the operator does not initiate the primary Feed and Bleed	5.5E-10
LOMFW_A	The AAD [SSS] system fails **then** the ASG [EFWS] fails due to a CCF **and finally** the primary Feed and Bleed fails after a successful manual initiation	4.0E-10
LOMFW_A	The AAD [SSS] system does not start due to an I&C failure **then** the ASG [EFWS] fails **and finally** the operators do not initiate primary bleed	3.4E-10

All the dominant accident sequences contain similar events. Following the failure of the normal SG feed systems, ARE [MFWS] and/or AAD [SSS], due to a CCF, there are two scenarios which result in core damage:

- The ASG [EFWS] is unavailable or fails during operation. After 2 hours the SGs empty. The operator then fails to initiate primary RHR. There is no residual heat removal and core damage occurs.

- The VDA [MSRT] valves are unavailable. The secondary side residual heat removal function is provided by the Main Steam Safety Valves (MSSV) but, in this case, it is impossible to initiate a primary cooldown allowing connection of the RHR system to the RCP [RCS]. After six hours, if the operator fails to initiate make-up to the ASG [EFWS] tanks these tanks are empty and the SGs start emptying. When the SGs are empty the operator should actuate the Feed and Bleed operation. If he fails to do this, core damage occurs.

Each accident sequence ends with the failure of the primary residual heat removal via Feed and Bleed which is the ultimate back-up for performing the RHR function. This ultimate cooling method is fully independent of the secondary systems and can be used for all the above scenarios.

The I&C systems are important for the operation of the ASG [EFWS] and the VDA [MSRT]. However, since the PSA conservatively assumes no operator recovery from I&C failures for VDA, the importance of I&C failures is over-estimated.

5.6.4. Initiating Events Analysis

5.6.4.1. Total Loss of Main Feedwater (LOMFW)

5.6.4.1.1. Event Description

The initiating event “Loss of Main Feedwater” corresponds to a total failure of the ARE [MFWS] system in operation during at-power state (state A) i.e. the SGs are no longer fed by the ARE [MFWS].

Following failure of the ARE [MFWS], the inventory of the steam generators decreases while the core power remains the same and the reactor coolant system pressure and temperature increase.

Reactor trip is automatically actuated following a “low steam generator level” or “low departure from nucleate boiling ratio” signal. The main feedwater full load isolation valve is closed by the reactor trip signal. At the same time, the AAD [SSS] pump starts automatically following a “ARE pumps off” signal. The capacity of the AAD [SSS] pump is insufficient to maintain the SG level at full power but it is sufficient with a good margin following the reactor trip. Following trip, the residual heat removal function could be provided using the main steam bypass. However, it is conservatively assumed that the MSIV are automatically closed.

Following MSIV closure, the steam is released to the atmosphere through the VDA [MSRT]. The operator initiates a secondary cooldown to reach the RIS-RA [RHR] connection conditions. The AAD/ARE [SSS/MFWS] tank inventory is sufficient to support this cooldown. The safe shutdown state is reached once the connection to the RIS-RA [RHR] has been performed.

5.6.4.1.2. Functional Safety Requirements

This section identifies which safety functions are challenged by a Loss of Main Feedwater:

- **Reactivity Control:** Reactivity control is provided by the reactor trip.

  The consequences of the failure of the rod drop are not considered in this section. They are considered in section 5.10 of this sub-chapter on Anticipated Transients Without Scram.

- Removal of core decay heat and stored heat. This safety function is divided into:

  - **Residual heat removal:** The residual heat removal function is provided by the SGs. They are fed by the AAD [SSS] system which is started automatically following a “ARE [MFWS] pumps off signal. Steam is dumped to the atmosphere through the VDA [MSRT].

If the AAD [SSS] fails, the ASG [EFWS] starts automatically when the “low low SG level” setpoint is reached.

- If the VDA [MSRT] fail to open, the Main Steam Safety Valves (MSSV) control the SG pressure and maintain it at about 105 bars. These valves cannot be used for the plant cooldown to RIS-RA [RHR] connection conditions. To maintain RHR using the secondary side for the long term, make-up to the ARE/AAD [SSS/MFWS] tank or cross-connection of the ASG [EFWS] tanks has to be carried out by the operator.

- If the secondary side RHR fails, a primary side RHR using Feed and Bleed is initiated by the operator. To achieve this, the Primary Depressurisation Valves or the Pressuriser Safety Valves are opened and the safety injection system (RIS [SIS]) is started.
    - **Long term cooling:** The long term cooling is provided by the RIS-RA [RHR] system or the containment heat removal system (EVU [CHRS]) during Feed and Bleed.
- **Reactor Coolant System integrity:** The RCP [RCS] integrity is challenged in the event of Feed and Bleed operation. Feed and Bleed operation requires the operator to open of the Pressuriser valves.
- **Reactor Coolant System inventory control:** The RCP [RCS] inventory control function is challenged by Feed and Bleed operation. This safety function is provided by the Medium Head Safety Injection (MHSI) trains.

5.6.4.1.3. Detailed Results

The “Loss of Main Feedwater” represents **1.6% of the Internal Event CDF, with a frequency of 8.4E-09/r.y.**

The following table lists the main accident sequences. Each accident sequence corresponds to one or a group of MCSs. The main accident sequences listed in the table below represent 98% of the initiating event risk.

Initiating event	***Brief description of the accident sequence***	***Frequency (per reactor per year)***
LOMFW_A	The AAD [SSS] system fails **then** the ASG [EFWS] fails due to a CCF **and finally** the operators do not initiate primary bleed	4.6E-09
LOMFW_A	Total digital I&C failure causes the loss of the VDA [MSRT] and AAD [SSS] systems **then** operator fails to manually control the ASG [EFWS] **and finally** the primary Feed and Bleed fails	1.8E-09
LOMFW_A	The AAD [SSS] system fails **then** the ASG [EFWS] fails due to an I&C failure and the operator fails to manually control the ASG [EFWS] **and finally** the operators do not initiate primary bleed	9.3E-10
LOMFW_A	The AAD [SSS] system fails **then** the ASG [EFWS] fails due to a CCF **and finally** the primary Feed and Bleed fails after a successful manual initiation	4.0E-10
LOMFW_A	The AAD [SSS] system does not start due to an I&C failure **then** the ASG [EFWS] fails **and finally** the operators do not initiate primary bleed	3.4E-10

Initiating event	***Brief description of the accident sequence***	***Frequency (per reactor per year)***
LOMFW_A	An I&C or mechanical failure causes the loss of the VDA [MSRT] **then** the operators do not initiate the make-up of the AAD/ARE [SSS/MFWS] tank **and finally** the operators do not initiate primary bleed	2.3E-10

The following systems are important in the protection against “Loss of Main Feedwater”:

- The **ASG [EFWS] system**. The ASG [EFWS] system is risk significant because it is the back-up to the AAD [SSS] system which has a low reliability. Consequently the frequency of a demand on the ASG [EFWS] is high.

- The **AAD [SSS] system**. The AAD [SSS] system is risk significant because, if it operates, the SGs are fed and the failure of ARE [MFWS] is mitigated.

The following I&C systems are important in providing protection against “Loss of Main Feedwater”:

- The **PS system**. This I&C system is important, because its failure makes the ASG [EFWS] and the VDA [MSRT] valves unavailable.

- The **SPPA-T2000 platform**. Failure of this platform makes the starting of AAD [SSS] impossible.

The following operator actions are important in the protection against “Loss of Main Feedwater”:

- The event “**Operator fails to initiate primary bleed**” contributes to most of the dominant minimal cut sets. This event is the most probable of all the primary RHR failure causes and primary RHR is the ultimate cooling means in all accident sequences.

- The event “**Operator fails to start and control EFWS**” is important. Indeed, the operator can provide a backup for the automatic start-up or control of the EFWS when the system is available.

- The event “**Operator fails to initiate ASG [EFWS] cross-connection or ARE/AAD [MFWS]/[SSS] tank make-up**” is important. The make-up initiation or the cross connection are the only back-up to failure of the VDA [MSRT].

  It should be noted that if the four ASG [EFWS] trains are in operation, the cross-connection of the ASG [EFWS] tanks is not necessary. For modelling simplification reason the PSA assumes conservatively that the cross-connection is required.

5.6.4.2. Loss of Start-up and Shutdown System (LOSSS)

5.6.4.2.1. Event Description

The initiating event “Loss of Start-up and Shutdown System AAD [SSS]” corresponds to a total failure in operation of the AAD [SSS] during intermediate shutdown state B when it provides the normal steam generator water make-up.

This initiating event can only occur in intermediate shutdown state B. Therefore, the plant is already tripped. Following failure of the AAD [SSS] system, the SGs start emptying slowly. The thermal power of the core is much lower than that considered in the “Loss of Main Feedwater” event. Following failure of the AAD [SSS], the operator must start the ARE [MFWS] system to re-supply the SGs.

When the ARE [MFWS] runs, the secondary side RHR function is provided using the Main Steam Bypass (GCT [MSB]).

If the GCT [MSB] fails, the operator initiates a secondary cooldown using the VDA [MSRT] to reach the RIS-RA [RHR] connection conditions. The ARE/AAD [MFW/SSS] tank inventory is sufficient for this secondary cooldown.

5.6.4.2.2. Functional Safety Requirements

This section identifies which safety functions are challenged by a Loss of Start-up and Shutdown System:

- **Reactivity control:** The “Loss of Start-up and Shutdown System” is considered in state B. Consequently, the plant is already tripped and reactivity control is not a concern. The combination of the control rods and the boric acid concentration maintain a sufficient negative reactivity margin to reach the RIS-RA [RHR] connection condition.

- Removal of core decay heat and stored heat. This safety function is divided into:

  - **Residual heat removal:** The residual heat removal function is provided by the SGs. They are fed by the ARE [MFWS] system if it has been put in service by the operator. If the operator fails to, or the ARE [MFWS] system fails, the “low low SG level” signal setpoint is reached. This signal automatically starts the Emergency Feedwater System (ASG [EFWS]). The Main Steam Isolation Valves (MSIV) are assumed to be closed and hence the steam is released to the atmosphere through the VDA [MSRT].

    If the VDA [MSRT] fails to open following a “Loss of Main Feedwater”,, depressurisation of the RCP [RCS] is not possible. However, the ASG [EFWS] tank and/or ARE/AAD [MFW/SSS] tank inventory is sufficient for make-up to them to be disregarded as the residual power during reactor state B is low.

If the secondary side RHR fails, primary side RHR using Feed and Bleed is initiated by the operator.

  - **Long term cooling:** The long term cooling function is provided in the same way as for the “Loss of Main Feedwater System” event.

- The **Reactor Coolant System integrity** and the **Reactor Coolant System inventory control** functions are also provided in the same way as for the “Loss of Main Feedwater System” event discussed in sub-section 5.6.4.1 of this sub-chapter.

5.6.4.2.3. Detailed Results

The “Loss of Start-up and Shutdown System” represents **0.4% of the Internal Event CDF with a frequency of 2.2E-09/r.y.**

The following table lists the main accident sequences. Each accident sequence corresponds to one or a group of MCSs. The main accident sequences listed in the table below represent 96% of the initiating event risk.

Initiating event	***Brief description of the accident sequence***	***Frequency (per reactor per year)***
LOSSS_B	The ASG [EFWS] fails to start due to an I&C failure **and** the operator fails to manually control ASG [EFWS] and to start ARE [MFWS] **and finally** the operators do not initiate primary bleed or IRWST cooling	1.7E-09
LOSSS_B	The ARE [MFWS] system fails to start due to a CCF with the AAD [SSS] system **and** the ASG [EFWS] fails to run due to a CCF **and finally** the operator fails to initiate primary Feed and Bleed	1.5E-10
LOSSS_B	The ASG [EFWS] fails in operation due to an I&C failure **and** the operator fails to manually control ASG level and to start ARE [MFWS] **and finally** the operators do not initiate primary bleed	1.4E-10
LOSSS_B	The ARE [MFWS] system fails to start due to an I&C failure **and** the ASG [EFWS] fails due to a CCF **and finally** the operator fails to initiate primary Feed and Bleed	6.6E-11

The most risk significant events for the loss of AAD [SSS] are of the same as for the loss of ARE [MFWS], i.e.:

- **Operator actions to initiate Feed and Bleed or to control the ASG [EFWS]** in the case of automatic control failure,

- **ASG [EFWS] common cause failures**.

- The **PS system failure**, resulting in unavailability of the ASG [EFWS] and VDA [MSRT] valves.

- The **SPPA-T2000 platform failure**, making start-up of the ARE [MFWS] impossible.

The most risk significant system not considered in the event of Loss of Main Feedwater is:

- the "**ARE [MFWS] system fails due to a functional dependency with the initiating event**". The event probability corresponds to the conditional failure probability of the ARE [MFWS] when the AAD [SSS] fails. It is high as these two systems share the same tank, the same Electrical supply and pipes. This event is present in some sequences because of its high failure probability.

5.6.4.3. Turbine Trip (TT)

5.6.4.3.1. Event Description

The initiating event “turbine trip” corresponds to an abrupt closure of the turbine admission valves and to an opening of the Main Steam Bypass (GCT [MSB]) during at-power operation (reactor state A).

Immediately following the turbine trip, an automatic partial reactor trip is actuated. This partial trip is designed to improve the plant availability. Thus, within only a few seconds, the balance between the heat generated in the core and heat removal via the steam generators is re-established. By these countermeasures a reactor trip is avoided and the possibility of rapid start-up is maintained.

In the PSA, the partial trip is conservatively ignored. Its failure is assumed to occur in all cases. Following failure of the partial trip, the reactor trip is automatically actuated either following a high pressuriser pressure or on high steam generator pressure signal. The steam produced in the steam generators is dumped to the condenser via the Main Steam Bypass.

Subsequently, the controlled state is reached, defined in this case as the hot shutdown state, with residual heat being removed via the Main Steam Bypass. Feedwater supply is provided by the Main Feedwater System (ARE [MFWS]).

Note: a loss of offsite power could be caused by a Turbine Trip. This event is analysed with the LOOP events in sub-section 5.7 of this subchapter.

5.6.4.3.2. Functional Safety Requirements

The safe state is reached if the Main Steam Bypass succeeds in removing residual heat to the condenser, and if the ARE [MFWS] or AAD [SSS] systems succeed in feeding the SGs.

If one of these systems fails, closure of the Main Steam Isolation Valves (MSIV) is assumed. In this case the safe state is defined as the shutdown state (connected to the RIS-RA [RHR]).

Following MSIV closure, the plant response is as described in the following paragraphs.

- **Reactivity Control:** Reactivity control is provided by the reactor trip.

  The consequences of the failure of the rod drop are not considered in this section. They are analysed in section 5.10 of this sub-chapter on Anticipated Transient Without Scram.

- Removal of core decay heat and stored heat. This safety function is divided into:

  - **Residual heat removal.** The residual heat removal (RHR) function is provided by the SGs. The steam is released to the atmosphere through the VDA [MSRT]. The SGs are fed either with the ARE [MFWS] system or with the AAD [SSS] system that starts automatically on an “ARE pumps off” signal.

    If the AAD [SSS] and ARE [MFWS] systems fail, the ASG [EFWS] system starts automatically when the “low low SG level” setpoint is reached.

If the VDA [MSRT] valves fail to open following a “Loss of Main Feedwater”, depressurisation of the RCP [RCS] is not possible and ARE/AAD [MFWS/SSS] tank make-up or ASG tanks cross connection is required.

If the secondary side RHR fails, primary side RHR, using Feed and Bleed, is initiated by the operator.

- o **Long term cooling.** Long term cooling is provided in the same way as for the “Loss of Main Feedwater System” event.

- The **Reactor Coolant System integrity** and the **Reactor Coolant System inventory control** functions are also provided in the same way as for the “Loss of Main Feedwater System” event discussed in sub-section 5.6.4.1 of this sub-chapter.

5.6.4.3.3. Detailed Results

“Turbine trip” represents **0.8% of the Internal Event CDF with a frequency of 4.3E-09/r.y.**

The following table lists the main accident sequences. Each accident sequence corresponds to one or a group of MCSs. The main accident sequences listed in the table below represent 99% of the initiating event risk.

Initiating event	***Brief description of the accident sequence***	***Frequency (per reactor per year)***
TT_A	ARE [MFWS] and AAD [SSS] fails due to total loss of digital I&C **and** the operator fails to manually control the ASG [EFWS] **and finally** the operator fails to initiate the primary Feed and Bleed or to initiate IRWST cooling with EVU [CHRS]	4.1E-09
TT_A	Main Steam Bypass fails **and** an I&C failure causes the failure of the VDA [MSRT] valves **and** the operator fails to initiate make-up to the tanks **and finally** the operator fails to initiate the primary Feed and Bleed	9.1E-11
TT_A	ARE [MFWS] and AAD [SSS] fail due to a common cause **and** ASG [EFWS] fails due to a CCF **and finally** the operator fails to initiate the primary Feed and Bleed	2.0E-11

Some of the most risk significant events for turbine trip are the same as those for Loss of Main Feedwater, i.e.:

- Operator actions i.e. **Feed and Bleed operation, manual control of ASG [EFWS]**: The manual control of the ASG [EFWS] through the NCSS is an important action within this group. The ASG [EFWS] is automatically started, but not controlled, by the NCSS. Due to the fail-safe position of the power control valve, SG feed is ensured after automatic start-up of the ASG [EFWS]. Nevertheless, this is conservatively neglected in the present PSA, which increases the importance of this action.

- **ASG [EFWS] common cause failures**.

- The **PS system failure**, resulting in unavailability of ASG [EFWS] and VDA [MSRT] valves.

- The **SPPA-T2000 platform failure**, making start-up of ARE [MFWS] and AAD [SSS] impossible.

5.6.4.4. Loss of Condenser (LOC)

5.6.4.4.1. Event Description

The initiating event “Loss of Condenser” corresponds to the failure to maintain the condenser vacuum.

When the pressure in the condenser reaches a certain level, a “low-vacuum trip” signal is generated, actuating a turbine trip. When the pressure reaches a higher threshold, a bypass trip is actuated, leading to unavailability of the main steam bypass. The consequential loss of steam flow from the secondary side causes a rapid increase in the SGs pressure and in the reactor coolant system (RCS) pressure.

Turbine trip is mitigated by a fast automatic reduction of reactor power by the partial trip. This counter measure is not claimed, and in the present analysis the partial trip is always assumed to fail. Consequently, the reactor trip is automatically actuated following either a high steam generator pressure or a high pressuriser pressure signal. The MFWS Full Load Isolation Valves are closed following the reactor trip signal.
It is assumed that the Main Steam Isolation Valves (MSIV) are automatically closed. The operator initiates a secondary cool-down using the VDA [MSRT] to reach the RIS-RA [RHR] connection conditions. The ARE/AAD [MFWS/SSS] tank inventory is sufficient for this cool-down.

The safe state is reached when RHR using the RIS-RA [RHR] is effective.

Note: a loss of offsite power could be caused by the Loss of Condenser. This event is analysed together with the LOOP events in section 5.7 of this sub-chapter.

5.6.4.4.2. Functional Safety Requirements

Following a “Loss of Condenser”, the **reactivity control**, the **residual heat removal**, the **long term cooling,** the **Reactor Coolant System integrity** and the **Reactor Coolant System inventory control** functions are provided in the same way as for the MSIV closure following turbine trip event discussed in sub-section 5.6.4.3 of this sub-chapter .

5.6.4.4.3. Detailed Results

The “Loss of Condenser” represents **0.6% of the Internal Event CDF with a frequency of 3.1E-09/r.y.**

The following table lists the main accident sequences. Each accident sequence corresponds to one or a group of MCSs. The main accident sequences listed in the table below represent 98% of the initiating event risk.

Initiating event	***Brief description of the accident sequence***	***Frequency (per reactor per year)***
LOC_AB	The ARE [MFWS] and AAD [SSS] fail due to total loss of digital I&C **and** the operator fails to manually start and control the ASG [EFWS] **and finally** the operator fails to initiate the primary Feed and Bleed or to initiate IRWST cooling with EVU [CHRS]	2.3E-09
LOC_AB	An I&C failure or a mechanical CCF causes the failure of VDA [MSRT] valves **then** the operator does not initiate make-up to the tanks **and finally** the operator does not initiate the primary Feed and Bleed	5.5E-10
LOC_AB	The ARE [MFWS], AAD [SSS] and ASG [EFWS] systems fail due to a total digital I&C failure **and then** the operators fail to manually start the ASG [EFWS] and to initiate primary Feed and Bleed due to NCSS failure	1.5E-10
LOC_AB	A simultaneous failure of ARE [MFWS] and AAD [SSS] due to a common cause **and** a failure of ASG [EFWS] due to CCF **and finally** the operator fails to initiate the primary Feed and Bleed	1.2E-11

The most risk significant events for the Loss of Condenser (LOC) are **the same as for the turbine trip** event except the “failure of Main Steam Bypass” event which is not relevant to the Loss Of Condenser event.

5.7. LOSS OF OFFSITE POWER (LOOP)

5.7.1. Group Description

The assessment of the Loss Of Offsite Power (LOOP) initiating event is performed for two types of LOOP event considering short (< 2 hours) and long term (up to 24 hours) duration LOOP.

Loss Of Offsite Power is defined as loss of both the main and auxiliary grid connections. Automatic switchover to house load operation is conservatively assumed to fail with a probability of 1.

This analysis covers also the Station Black Out (SBO) situations. SBO is defined as Loss Of Offsite Power with unavailability of all four Emergency Diesel Generators (EDG).

The following initiating events are considered in the LOOP group:

- Short term LOOP in the at-power state A&B (LOOPS AB). This includes the LOOP event caused by a reactor trip (consequential LOOPS AB).
- Short term LOOP in shutdown state Ca (LOOPS Ca).
- Short term LOOP in shutdown state Cb (LOOPS Cb).
- Short term LOOP in shutdown state D (LOOPS D).
- Long term LOOP in power state AB (LOOPL AB). This includes the LOOP event caused by a reactor trip (consequential LOOPL AB).
- Long term LOOP in shutdown state Ca (LOOPL Ca).
- Long term LOOP in shutdown state Cb (LOOPL Cb).
- Long term LOOP in shutdown state D (LOOPL D).

A consequential Loss Of Offsite Power is defined as a loss of main and auxiliary grid connections due to the reactor trip following non-LOOP initiating events such as spurious reactor trip, turbine trip, Loss of Condenser or Loss of Main Feedwater.

The definitions and frequencies of the initiating events are given in section 4 of this sub-chapter.

5.7.2. Results

The contribution of the LOOP group to the **Internal Event Core Damage Frequency is 1.5E- 07/r.y**, which represents **27.9% of the Internal Event CDF**.

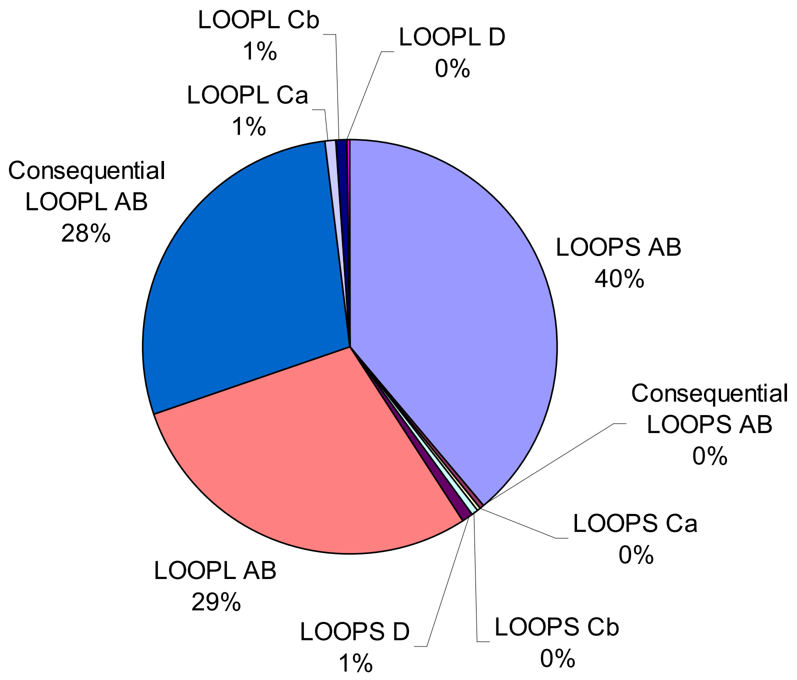
The core damage frequency of the LOOP group is approximately 1.5E-07 /r.y. Therefore LOOP does not represent a high contribution to the risk, even though the EPR is designed with active safety systems.

The CDF of each LOOP initiating event of the group is shown in the following table:

Initiating Event (IE)	IE frequency (/y)	CDF (/r.y)
Short Term Loss Of Offsite Power (<2 hours):		
LOOPS AB	6.00E-02	5.74E-08
Consequential LOOPS AB	4.87E-04	4.60E-10
LOOPS Ca	3.90E-04	4.96E-10
LOOPS Cb	5.50E-04	7.08E-10
LOOPS D	3.00E-04	1.18E-09
Long Term Loss Of Offsite Power (<24 hours):		
LOOPL AB	1.00E-03	4.30E-08
Consequential LOOPL AB	9.75E-04	4.19E-08
LOOPL Ca	6.50E-06	8.94E-10
LOOPL Cb	9.10E-06	1.27E-09
LOOPL D	5.00E-06	2.41E-10
total		**1.48E-07**

The partitioning of the CDF between power and shutdown is 97% for at-power states (A, B), including consequential LOOP and 3% for shutdown states (Ca, Cb, D).

The relative contribution of each LOOP initiating event within the group is given below:



5.7.3. Dominant Accident Sequence Analysis

The following table lists the main accident sequences of the LOOP group. They represent around 91% of the overall group CDF.

Initiating event (IE)	*Brief description of the main sequence analysis*	*Frequency (per reactor per year)*
LOOPL AB Consequ. LOOPL AB	The IE is followed by failure of the four EDG and • failure of the two SBO diesels, including operator failure to start the SBO diesels or • failure of the ASG [EFWS] trains supplied by SBO diesels.	5.0E-08
LOOPS AB Consequ. LOOPS AB	The IE is followed by the failure of the Reactor Coolant Pump seals and DEA [SSSS] **and** the failure of partial secondary cooldown due to I&C failure	3.9E-08
LOOPL AB Consequ. LOOPL AB	The IE is followed by a failure of the four EDG (SBO situation) **and** failure of the Reactor Coolant Pump seals **and** • failure to operate within the pressure and temperature envelope for DEA [SSSS] protection (i.e. which prevents correct DEA [SSSS] operation) **and** operator fails to initiate fast secondary cooldown (complete dependency conservatively assumed) or • mechanical failure of the DEA [SSSS] **and** failure of the initiation of fast secondary cooldown by the operator	1.6E-08
LOOPS AB Consequ. LOOPS AB	The IE is followed by the failure of secondary side feed with ASG [EFWS] **and** the failure of the initiation of Feed and Bleed by the operator (Feed and Bleed is considered after the recovery of the off-site grid).	1.1E-08
LOOPL AB Consequ. LOOPL AB	The IE is followed by a failure of the Reactor Coolant Pump seals **and** the failure to inject with the MHSI after a successful partial cooldown **thus** the fast cooldown fails due to operator failure or mechanical failures.	1.0E-08
LOOPS AB Consequ. LOOPS AB	The IE is followed by the failure of the Reactor Coolant Pump seals and DEA [SSSS] **and** the failure of MHSI injection due to electrical failure **and** the failure of fast secondary cooldown (including operator failure and system operation failure)	7.9E-09

The LOOP events show the relative importance of the electrical supply. However, with four Emergency Diesels Generators (LH-Diesels) (EDG) and two Station Blackout Diesel Generators (LJ-Diesels) (SBO-DG), the contribution of loss of power to the Internal Events CDF remains in the acceptable range.

Long Loss Of Offsite Power:

The sequences arising from the Long term LOOP in at-power states represent approximately 59% of the CDF for this group. The breakdown of the CDF between consequential LOOP and LOOP as an initiating event is almost 50-50.

During shutdown states, the long term LOOP contributes less than 2% of the CDF for the group, the risk of consequential seal LOCA is low and both steam generators (except for state D) and RHR systems are able to remove the residual heat.

For long term LOOP, the diesels are the most important components. Each function contributing to the residual heat removal requires the operation of at least one of the four Emergency Diesel Generators, or one of the two SBO Diesel Generators.

Short term Loss Of Offsite Power:

For the short term LOOP in at-power states, the Reactor Coolant Pump Seals and the DEA [SSSS] are particularly important because their failure causes a small LOCA.

Two diverse sets of batteries have been modelled in the UK EPR PSA; the common cause failure of the four batteries is considered as a sensitivity study in Sub-chapter 15.7. Failure of the two sets of batteries results in the unavailability of the electrical supply to the I&C and the actuators. The PSA assumes core damage would occur in this situation.

During shutdown states, the short term LOOP contributes less than 2% of the CDF for the group, the risk of consequential seal LOCA is low and both steam generators (except for state D) and the RHR systems are able to remove the residual heat.

5.7.4. Initiating Events Analysis

The following apply for each initiating event of the LOOP group:

- The Emergency Diesel Generators are automatically started, while the Station Blackout Diesels are usually started by the operator from the Main Control Room (MCR). Both starts require the availability of the batteries, the 220V uninterrupted power supply;

- The reloading sequence, which follows the start of the Emergency Diesel Generators, maintains the power supply to the safety trains and their support systems. The following systems are supported by this action: the Emergency Feedwater System (ASG [EFWS]), the Component Cooling Water System (RRI [CCWS]), and the Essential Service Water System (SEC [ESWS]), the Chemical and Volume Control System (RCV [CVCS]), the Safety Injection System (RIS [SIS]) and the Containment Heat Removal System (EVU [CHRS]);

- If the batteries fail, the Station Blackout Diesel Generators can be started manually by local action. This backup is only considered when the batteries fail in operation after a long time window.

5.7.4.1. Short Loss of Offsite Power (LOOPS)

5.7.4.1.1. Event Description: short term LOOP in power operation, States A&B

This section covers short term Loss Of Offsite Power in at-power states. The short term LOOP is defined as the maximum duration which can be survived without any electrical supply from the diesels or the grid.

This period is limited to 2 hours by:

- The water inventory of the steam generators which will provide approximately 1 hour 30 minutes of steaming through the Main Steam Safety Valves (MSSV) or Main Steam Relief Train (VDA [MSRT]) without feeding, followed by
- RCP [RCS] heatup with cycling of the Pressuriser Safety Valves for about 30 minutes.

Consequently, the short term LOOP event does not explicitly require the Emergency Diesel Generators (EDG) to start. The 2-hour batteries are required for the 2-hour LOOP to supply the LV- busbars for Instrumentation and Control (I&C) and for operation of the Main Steam Relief Trains (VDA [MSRT]). Unavailability of those busbars is mainly caused by failure of the 2-hour batteries and the failure of the operator to start the SBO diesels manually to supply the busbars (following the failure in operation of the batteries). However, as soon as the power is recovered, the core recovery is only possible with the manual actuation of Feed and Bleed. Indeed, the steam generators are dry on the secondary side and refilling of hot and dry steam generators is usually not foreseen in the emergency operating procedures.

5.7.4.1.2. Functional Safety Requirements: short term LOOP in power operation, States A&B

This section discusses the safety functions which are challenged by the short term LOOP event in at-power states:

- **Reactivity Control**: Reactivity control in the transient is provided by the rod drop following the reactor trip signal.

  The consequences of the failure of the rod drop are not considered in this section. They are considered in section 5.10 of this sub-chapter on Anticipated Transients Without Scram.

- Removal of core decay heat and stored heat. This safety function is divided into:

  - **Residual Heat Removal**: Residual heat removal is provided by the opening of the VDA [MSRT] or the Main Steam Safety Valves to remove the steam produced in the steam generators. Feeding of the steam generator with the Emergency Feedwater System is not explicitly required in the 2-hour LOOP. The water inventory present in the steam generators before the initiating event is sufficient. However, water makeup to the steam generators is considered in the event tree modelling to avoid Feed and Bleed.

    Following the failure of the steam generators, the heat is removed by Feed and Bleed. This requires an operator action and the availability of the Pressuriser Safety Valves or Primary Depressurisation Valves and of the Safety Injection System (RIS [SIS]).

  - **Long term cooling**: In the event of Feed and Bleed, long term cooling is provided by the cooling of the IRWST. This cooling is performed by the LHSI or the Containment Heat Removal System (EVU [CHRS]).

- **Reactor Coolant System integrity**: The Reactor Coolant System (RCP [RCS]) integrity could be challenged by a failure of the Reactor Coolant Pump seals.

  The Reactor Coolant Pump seal integrity is maintained by seal injection via the Chemical and Volume Control System (RCV [CVCS]) and by the thermal barrier cooled by the Component Cooling Water System (RRI [CCWS]). When the Reactor Coolant Pumps stop after the loss of the power supply, the Stand Still Seal System (DEA [SSSS]) maintains RCP [RCS] integrity with high reliability when the RCP [RCS] temperature and pressure remain within the design envelope.

- **Reactor Coolant System inventory control**: This is only required if the Reactor Coolant Pump seals fail. In this case it is necessary to control the RCP [RCS] inventory by using the Medium Head Safety Injection (MHSI) Pumps. This requires the start of at least one Emergency Diesel Generator to supply the MHSI.

  Prior to MHSI injection, the pressure in the RCP [RCS] must be reduced using the secondary side, by opening the VDA [MSRT] to achieve a partial cooldown.

5.7.4.1.3. Event Description: short term LOOP in shutdown, LOOPS - Ca, Cb and D

This section covers short term Loss Of Offsite Power in the shutdown states.

For state C (Ca and Cb), the 2-hour duration is linked to the capacity of the batteries. With the reactor shutdown, the steam generator inventory is sufficient to provide cooling for much longer than 2 hours. However, after 2 hours without any power supply, the VDA [MSRT] will close, preventing the removal of residual heat.

For state D, 2 hours is the maximum time allowable without MHSI or LHSI pumps for RHR or makeup. The first automatic or manual action must be performed within two hours.

5.7.4.1.4. Functional Safety Requirements: short term LOOP in shutdown, LOOPS - Ca, Cb

This section discusses the safety functions which are challenged by the short term LOOP event in states Ca and Cb:

- **Reactivity Control**: Reactivity control is not challenged by the transient.

- Removal of core decay heat and stored heat. This safety function is divided into:

  - **Residual Heat Removal**: Residual heat removal is provided firstly by the automatic restart of the Residual Heat Removal (RHR) trains previously in operation. The RHR function requires the EDG power supply. The RHR train(s) in standby can also be started from the control room by the operator.

In the event of RHR failure in state C (Ca and Cb), residual heat is removed by the automatic opening of the VDA [MSRT] at their setpoint for cold shutdown. This discharges steam produced in the steam generators. Failure of heat removal via the secondary side leads to core damage. The PSA does not consider Feed and Bleed for short term LOOP in the event of the failure of secondary side heat removal.

Feeding of the steam generator with the ASG [EFWS] is not required in the 2-hour LOOP. The water inventory in the steam generator before the initiating event is sufficient.

  - **Long term cooling**: Long term cooling is not considered for short term LOOP.

- **Reactor Coolant System integrity**: The RCP [RCS] integrity is not challenged by the initiating event. The integrity of the Reactor Coolant Pump seals is not challenged in cold shutdown.

  Reactor Coolant System inventory control: RCP [RCS] inventory control is not challenged in the transient.

5.7.4.1.5. Functional Safety Requirements: short term LOOP in shutdown, LOOPS D

This section discusses the safety functions which are challenged by the short term LOOP event in state D:

- **Reactivity Control**: Reactivity control is not challenged by the transient. Makeup for safety injection uses borated water.

- Removal of core decay heat and stored heat. This safety function is divided into:

  - **Residual Heat Removal**: Residual heat removal is provided first by the automatic restart of the Residual Heat Removal (RHR) trains previously in operation. The RHR function requires EDG power supply. The RHR train(s) in standby can also be started from the control room by the operator.

    In the event of RHR failure in state D, the residual heat cannot be removed by the steam generator because the vessel head is off. Makeup is performed by the Safety Injection System to compensate for the steaming and to raise water level sufficiently to restart the RHR pumps.

  - **Long term cooling**: Long term cooling is not considered for the short term LOOP.

- **Reactor Coolant System integrity**: The RCP [RCS] integrity is not challenged by the initiating event. The RCP [RCS] is open.

- **Reactor Coolant System inventory control**: RCP [RCS] inventory control is required in the event of RCP [RCS] boiling following RHR failure. This function is automatically performed by the MHSI pumps, or manually with the LHSI pumps.

5.7.4.1.6. Detailed Results

The short term LOOP represents **11% of the Internal Event CDF with a frequency of 6.0E-08/r.y**. The consequential short term LOOP is negligible and represents significantly less than 1% (5E-10 /r.y).

The short term LOOP during power operation represents 96% of the CDF arising from short term LOOP events. The short term LOOP during shutdown represents 4% of the CDF.

The following table lists the main short term LOOP accident sequences. They represent around 99% of the risk from short term LOOP.

Initiating event	***Brief description of the accident sequences***	***Frequency (per reactor per year)***
LOOPS AB Consequ. LOOPS AB	The IE is followed by the failure of the Reactor Coolant Pump seals and DEA [SSSS] **and** the failure of partial secondary cooldown due to I&C failure	3.9E-08
LOOPS AB Consequ. LOOPS AB	The IE is followed by the failure of secondary side feed with ASG [EFWS] **and** the failure of the initiation of Feed and Bleed by the operator	1.1E-08
LOOPS AB Consequ. LOOPS AB	The IE is followed by the failure of the Reactor Coolant Pump seals and DEA [SSSS] **and** the failure of MHSI injection due to electrical failure **and** the failure of fast secondary cooldown (including operator failure and system operation failure)	7.9E-09
LOOPS Ca LOOPS Cb	The IE is followed by the failure of RHR (loss of all LHSI trains) due to a I&C failure **and** the failure of the initiation of secondary RHR	1.1E-09
LOOPS D	The IE is followed by the failure of the EDGs either due to mechanical failure or due to I&C failure (SBO situation) **and** makeup by LHSI fails (failure to start SBO diesels, or to start LHSI).	1.0E-09

The following systems are important in the protection against the short term LOOP:

- The **Diesels** (Emergency Diesel Generators LHP/Q/R/S and SBO Diesel Generator LJP/S). For short term LOOP they are required following the failure in operation of the batteries to support the I&C or to prevent initiation of Feed and Bleed by ensuring electrical supply to the ASG [EFWS] pumps.

  In the event of Reactor Coolant Pump seals failure, the diesels are required to provide electrical supplies for the safety injection pumps.

- The **Reactor Coolant Pump Seals** and the **DEA [SSSS]** are important because their failure causes a small LOCA. The DEA [SSSS] acts as backup of the seal.

- The **ASG [EFWS] system** which supports the removal of residual heat and avoid Feed and Bleed actuation.

- The **MHSI pumps** and the support system RRI/SEC [CCWS/ESWS]. These systems are required in the following cases:
  - The failure of the Reactor Coolant Pump seals in order to mitigate the small LOCA. All components are supplied by the EDGs.
  - The failure of the secondary side heat removal (for power state only). In this case, in order to perform Feed and Bleed, the primary feed by MHSI is required after the LOOP recovery and the MHSI are supplied by off-site power.

The following I&C signals or systems are important for providing protection against the short term LOOP:

- The **Protection System (RPR [PS])**. The protection system actuates numerous automatic actions, including the start of the Emergency Diesel Generators, the start of the ASG [EFWS] pumps, the opening of the Main Steam Relief Valves. The Protection System (RPR [PS]) also performs Partial Cooldown and Safety Injection following failure of the Reactor Coolant Pump seals.

  The **SPPA-T2000 platform**. This platform is needed for performing the following operator actions from the main control room: the start of SBO diesels, and the opening of VDA (MSRT).

The following operator actions are important in the protection against the short term LOOP:

- The **operator performs Feed and Bleed** in the event of failure of RHR via the steam generators.
- The **operator performs fast secondary cooldown** (power state) in the event of failure of MHSI injection, and the **operator starts secondary cooldown** (state C) in case of primary RHR failure.
- The **operator starts the SBO diesels**. This is performed from the Main Control Room or locally in the Diesel Building. The SBO diesels can be started without any electrical supply.
- The **operator starts a RHR train** (all shutdown states) and the **operator starts make up with LHSI** (shutdown state D). These actions are required following failure of the reloading sequence of the RHR train previously in operation. The main reason for this requirement would be the failure of all EDG. Those two actions enable residual heat removal.

5.7.4.2. Long Term Loss of Offsite Power (LOOPL)

5.7.4.2.1. Event Description: Long term LOOP in power operation, LOOPL AB

This section covers the Long term Loss Of Offsite Power in at-power states. The long term LOOP is assumed to last for 24 hours.

The long term LOOP mainly challenges the residual heat removal function. In the event of Reactor Coolant Pump seal LOCA, the inventory control function is also challenged.

5.7.4.2.2. Functional Safety Requirements: long term LOOP in power operation, LOOPL AB

This section describes the safety functions which are challenged by the long term LOOP event in at-power states:

- **Reactivity Control**: Reactivity control in the transient is provided by rod drop following the reactor trip signal.

  The consequences of the failure of the rods to drop are not considered in this section. They are considered in section 5.10 of this sub-chapter on Anticipated Transients Without Scram.

- Removal of core decay heat and stored heat. This safety function is divided into:

  - **Residual Heat Removal**: Residual heat removal is provided by the opening of the VDA [MSRT] or the Main Steam Safety Valves to discharge the steam produced in the steam generators. In the 24 hour LOOP, the Steam Generators need to be fed by the Emergency Feedwater System (ASG [EFWS]).

    In the event of failure of the steam generators, the heat is removed by Feed and Bleed. This requires an operator action and the availability of the Pressuriser Safety Valves or Primary Depressurisation Valves and of the Safety Injection System (RIS [SIS]).

  - **Long term cooling**: In the event of Feed and Bleed or Reactor Coolant Pump seals failure, see RCP [RCS] integrity, long term cooling is provided by the cooling of the IRWST. This cooling is performed by the LHSI or the Containment Heat Removal System.

- **Reactor Coolant System integrity**: The RCP [RCS] integrity could be challenged in the event of failure of the Reactor Coolant Pump seals.

  The integrity of the Reactor Coolant Pump seals is maintained by seal injection via the RCV [CVCS] and the thermal barrier cooled by the Component Cooling Water System. When the Reactor Coolant Pumps stop following the loss of power supply, the DEA [SSSS] ensures the RCP [RCS] integrity with high reliability. In SBO conditions, the RCP [RCS] pressure and temperature need to be slightly reduced after a few hours, in order to ensure the leak tightness of the DEA [SSSS]. This pressure and temperature reduction may require a manual opening of the VDA [MSRT] and a cross connexion of the SG feed lines in case of emergency diesel generators failure.

- **Reactor Coolant System inventory control**: In the event of failure of the Reactor Coolant Pump seals or in the event of Feed and Bleed, the inventory is controlled by the Safety Injection System. This requires the start of at least one diesel, an EDG or a SBO diesel, to supply the RIS [SIS] pumps.

  Prior to the SIS injection, the pressure must be decreased in the RCP [RCS] using the secondary side. This is achieved by opening the VDA [MSRT] for a partial cooldown or a fast secondary cooldown.

5.7.4.2.3. Event Description: long term LOOP in shutdown, LOOPL Ca, Cb and D

This section covers the long Loss Of Offsite Power in the shutdown states. The long term LOOP is a 24 hours loss of offsite power.

5.7.4.2.4. Functional Safety Requirements: long term LOOP in shutdown, LOOPL Ca, Cb

This section discusses the safety functions which are challenged by the long term LOOP event in states Ca and Cb:

- **Reactivity Control**: Reactivity control is not challenged by the transient.
- Removal of core decay heat and stored heat. This safety function is divided into:
  - **Residual Heat Removal**: Residual heat removal is provided firstly by the automatic restart of the Residual Heat Removal (RHR) trains previously in operation. The RHR function requires an EDG power supply. The RHR train(s) in standby can also be started from the control room by the operator.

    In the event of RHR failure in state C (Ca and Cb), the residual heat is removed by the automatic opening of the VDA [MSRT] at their setpoint for cold shutdown. They discharge the steam produced in the steam generators. The steam generators are fed by the ASG [EFWS] supported by the EDG or SBO diesels.
  - **Long term cooling**: In the event of long term LOOP in state C, only secondary side heat removal is considered for long term cooling.
- **Reactor Coolant System integrity**: The RCP [RCS] integrity is not challenged by the initiating event. The integrity of the Reactor Coolant Pump seals is guaranteed in cold shutdown.
- **Reactor Coolant System inventory control**: The RCP [RCS] inventory control function is not challenged in the transient.

5.7.4.2.5. Functional Safety Requirements: long term LOOP in shutdown, LOOPL D

This section discusses the safety functions which are challenged by the long term LOOP event in the state D:

- **Reactivity Control**: Reactivity control is not challenged by the transient.
- Removal of core decay heat and stored heat. This safety function is divided into:
  - **Residual Heat Removal**: Residual heat removal is provided firstly by the automatic restart of the Residual Heat Removal (RHR) trains previously in operation. The RHR function requires an EDG power supply. The RHR train(s) in standby can also be started from the control room by the operator.

    In the event of RHR failure in state D, the residual heat cannot be removed by the steam generator since the vessel head has been removed. Makeup is performed by the Safety Injection System. This compensates for the steaming and raises the water level sufficiently to restart the RHR trains.

- **Long term cooling**: Flooding of the reactor cavity provides long term cooling.

- **Reactor Coolant System integrity**: the RCP [RCS] integrity is not challenged by the initiating event. The RCP [RCS] is open.

- **Reactor Coolant System inventory control**: the RCP [RCS] inventory control function is automatically performed by the MHSI pumps or manually with the LHSI pumps. The RCP [RCS] makeup is required in the event of the RCP [RCS] boiling due to the RHR failure.

5.7.4.2.6. Detailed Results

The long term LOOP represents 16**% of the Internal Event CDF** with a **core damage frequency of 8.7E-08 /r.y**. The consequential long term LOOP represents 8% (4.2E-08 /r.y).

The long term LOOP in power operation represents 97% of the CDF due to long term LOOP. The long term LOOP in shutdown represents only 3% of the CDF.

The following table lists the main accident sequences of the Long term LOOP. They represent around 92% of the CDF of the Long term LOOP.

Initiating event	*Brief description of the accident sequences*	*Frequency (per reactor per year)*
LOOPL AB Consequ. LOOPL AB	The IE is followed by failure of the four EDG and • failure of the two SBO diesels, including operator failure to start the SBO diesels or • failure of the ASG [EFWS] trains supplied by SBO diesels.	5.0E-08
LOOPL AB Consequ. LOOPL AB	The IE is followed by a failure of the four EDG (SBO situation) **and** failure of the Reactor Coolant Pump seals **and** • failure to operate within the pressure and temperature envelope for DEA [SSSS] protection (i.e. which prevents correct DEA operation) **and** operator fails to initiate fast secondary cooldown (complete dependency conservatively assumed) or • mechanical failure of the DEA **and** failure of the initiation of fast secondary cooldown by the operator	1.6E-08
LOOPL AB Consequ. LOOPL AB	The IE is followed by a failure of the Reactor Coolant Pump seals **and** the failure to inject with the MHSI after a successful partial cooldown **thus** the fast cooldown fails due to operator failure or mechanical failures.	1.0E-08

Initiating event	***Brief description of the accident sequences***	***Frequency (per reactor per year)***
LOOPL AB Consequ. LOOPL AB	The IE is followed by a failure of secondary side heat removal **and** a failure of Feed and Bleed (operator failure to initiate Feed and Bleed or MHSI failure to feed).	2.6E-09
LOOPL Ca, LOOPL Cb	The IE is followed by a failure of the residual heat removal via primary or secondary side **and** a failure of the primary make-up after initiation of primary bleed. The main cause is a loss of the EDG and SBO diesels.	1.9E-09

The following systems are important in the protection against the long term LOOP:

- The **Diesels** (Emergency Diesel Generators LH- and SBO Diesel Generator LJ-). In long term LOOP, the diesels are required to supply the equipment involved in the residual heat removal function. This includes the ASG [EFWS] pumps or the RIS [SIS] pumps and the RRI/SEC [CCWS/ESWS] pumps.

  The diesels are also required to supply the I&C once the 2-hour batteries capacity limit has been exceeded.

- The **Reactor Coolant Pump seals** and **DEA [SSSS]**: are important because their failure causes a small LOCA. The DEA [SSSS] acts as a backup to the seal.

- The **ASG [EFWS]** pumps. The ASG [EFWS] system is the first system challenged for residual heat removal in the event of long term LOOP.

- The **MHSI pumps** and the **support system** (RRI/SEC [CCWS/ESWS]). These systems are required in the following cases:

  - the failure of the Reactor Coolant Pump seals in order to mitigate the small LOCA. All components are supplied by the EDGs.

  - the failure of primary and secondary side heat removal. In this case, in order to perform Feed and Bleed, the primary feed by MHSI is required.

The following I&C signal or system is important in providing protection against the long term LOOP:

- The **Protection System (RPR [PS])**. The protection system actuates numerous automatic actions, including the start of the Emergency Diesel Generators, the start of the ASG [EFWS] pumps, the opening of the Main Steam Relief Valves (MSRV). The Protection System (RPR [PS]) also performs Partial Cool-down and Safety Injection following failure of the Reactor Coolant Pump seals.

- The **SPPA-T2000 platform**. This platform is needed for performing numerous operator actions: the start of SBO diesels, the start of ASG [EFWS], the start of RHR train or RCS make-up, as well as the initiation of Feed and Bleed.

The following operator actions are important in the protection against long term LOOP:

- The **operator performs Feed and Bleed** in the event of failure of RHR via the steam generators.

- The **operator performs fast secondary cooldown** (power state) in the event of MHSI injection unavailability.

- The **operator starts the SBO diesel** (LJ-Diesels) from the Main Control Room or locally in the Diesel Building following failure of the 2-hour batteries.

- The **operator performs cooling in the event of a SBO** for Reactor Coolant Pump seals protection.

5.8. PRIMARY TRANSIENTS

5.8.1. Group Description

The Primary Transients group covers initiating events that cause Reactor Coolant System perturbations in normal operation. The transients are studied from the at-power state (state A) to cold shutdown with RCP [RCS] open (state D).

The following initiating events are considered in the group:

- Spurious Reactor Trip in at-power state A (RT_A-).
- Heterogeneous Dilution
- Heterogeneous Dilution in at-power state A (DIL HE_A)
- Heterogeneous Dilution in shutdown state Ca (DIL HE_CA).
- Homogeneous Boron Dilution
- Homogeneous Boron Dilution at 36 te/h from RBWMS in at-power state A (DIL HO--_A-).
- Homogeneous Boron Dilution at 100 te/h from RBWMS in intermediate shutdown state B (DIL HO100_B-).
- Homogeneous Boron Dilution at 72 te/h from RBWMS in shutdown state Ca (DIL HO72_CA).
- Homogeneous Boron Dilution at 36 te/h from RBWMS in shutdown state Cb (DIL HO36_CB).
- Homogeneous Boron Dilution at 36 te/h from RBWMS in shutdown state D (DIL HO36_D-).
- Homogeneous Boron Dilution at 15 te/h from heat exchanger leakages in intermediate shutdown state B (DIL HO15_B-).
- Homogeneous Boron Dilution at 15 te/h from heat exchanger leakages in shutdown state Ca (DIL HO15_CA).
- Homogeneous Boron Dilution at 15 te/h from heat exchanger leakages in shutdown state Cb (DIL HO15_CB).
- Loss of Residual heat removal System in operation:
- Loss of 4/4 LHSI/RHR trains in shutdown state Ca (LORHR_CA).
- Loss of 3/3 LHSI/RHR trains in shutdown state Cb (LORHR_CB)
- Loss of 3/3 LHSI/RHR trains in shutdown state D (LORHR_D).

- Uncontrolled Level Drop
- Uncontrolled Level Drop in shutdown state Cb (ULD--_CB).
- Uncontrolled Level Drop in shutdown state D (ULD--_D-).

The definition and frequencies of the initiating events are presented in section 4 of this sub-chapter. The frequencies are tabulated in the following section.

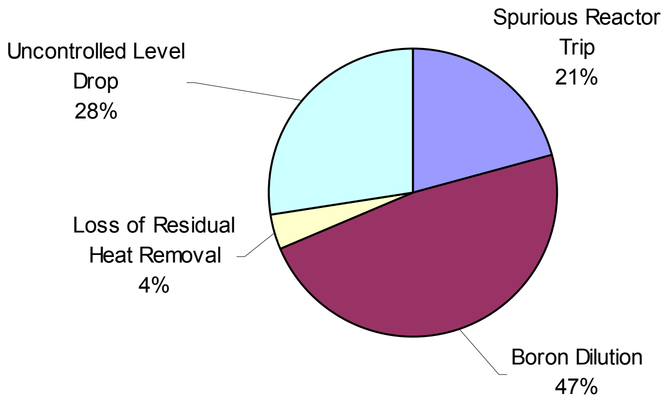
5.8.2. Results

The contribution of the primary transients group to the **Internal Event Core Damage Frequency is 8.17E-08/r.y**, which represents **15.4% of the Internal Event CDF**.

The contribution of each primary transient initiating event within the group is given below:

Initiating Event	IE frequency (/y)	CDF (/r.y)
Spurious Reactor Trip	{CCI}[a]	1.71E-08
Boron Dilution (sum)	{CCI}[a]	3.89E-08
Loss Of Residual Heat Removal (sum)	{CCI}[a]	3.22E-09
Uncontrolled Level Drop (sum)	{CCI}[a]	2.25E-08
Total		8.17E-08

The contribution of each initiating event to the CDF of the group is shown in the following figure:



5.8.3. Dominant Accident Sequences Analysis

The following table lists the main accident sequences of the primary transients group. Each accident sequence corresponds to one or a group of Minimal Cutsets (MCS). The main accident sequences presented in the table below contribute 86% to the overall group CDF.

Initiating event	***Brief description of the accident sequence***	***Frequency (per reactor per year)***
DIL HO100_B-	An I&C failure causes the failure of the prevent dilution signal and of the VCT isolation due to the failure of Anti Dilution signal **and** boration fails due to failure of the RBS [EBS] (pumps or train D discharge line) **and** the operator fails to isolate the source of dilution.	2.2E-08
RT_A-	ARE [MFWS] and AAD [SSS] fail due to total loss of digital I&C **and** the operator fails to manually control the ASG [EFWS] **and finally** the operator fails to initiate the primary Feed and Bleed or to initiate IRWST cooling with CHRS.	1.6E-08
ULD--_CB	I&C failures (RPR [PS] level measurements) cause the uncontrolled level drop, **and**, after automatic isolation of the draining path with NCSS, automatic makeup with MHSI trains fails due to failure of RIS [SIS] signals from RPR [PS] and SAS **and** failure of the manual makeup with RIS [SIS] trains due to operator failure.	9.6E-09
ULD--_CB	I&C failures (RPR [PS] level measurements) cause the uncontrolled level drop, **and**, after automatic isolation of the draining path with NCSS, automatic makeup with MHSI trains fails due to failure of RIS [SIS] signals from RPR [PS] and SAS **and** failure of the makeup with LHSI trains due to failure to trip the RHR pumps on low low loop level from RPR [PS] and failure of the fourth LHSI train due to mechanical failure (including support systems).	8.9E-09
DIL HE_CA	All scenarios of Heterogeneous Dilution in state Ca.	4.5E-09
DIL HO100_B-	Total failure of digital I&C causes the failure of the VCT isolation due to the failure of Anti Dilution signal **and** the failure of RBS [EBS] actuation.**and** the operator fails to isolate the source of dilution with NCSS.	4.4E-09
DIL HO--_A-	An I&C failure causes the failure of control rods due to the failure of the automatic control of Average Coolant Temperature and the failure of VCT isolation due to the failure of Anti Dilution signal **and** the operator fails to isolate the source of dilution.	1.7E-09
LORHR_CB	The secondary RHR fails following ASG [EFWS] and/or VDA [MSRT] failure and/or preventive maintenance on SG **and** the operator fails to start the fourth LHSI/RHR train **and** the operator fails to initiate primary Feed and Bleed.	1.6E-09
ULD--_CB	Failure of the automatic isolation of CVCS and automatic makeup with MHSI trains due to the failure of main and diversified Reactor Coolant System Level measurements **and** the operator fails to initiate the manual makeup with RIS [SIS] trains.	1.6E-09

The initiating events covered by the primary transient group differ widely with no significant common features.

Boron Dilution is the most important contributor to the core damage frequency for this group with boron dilution at-power state AB dominating. The mitigation of boron dilution relies on the detection and isolation of the dilution. No front line Safety System is directly challenged by the event, except boron injection by the RBS [EBS], which gives more time to isolate the dilution. It should be noted that the contribution from heterogeneous boron dilution is 6.4% of the primary transient group (5.2E-09/r.y).

Uncontrolled Level Drop is the second most important contributor to the core damage frequency for this group. The mitigation of uncontrolled level drop relies on the isolation of the RCV [CVCS] and on the initiation of water makeup by the RIS [SIS] trains.

Spurious reactor trip is also an important contributor to the core damage frequency for this group with a high initiating event frequency. The mitigation of spurious reactor trip relies on the residual heat removal by the secondary systems and in case of failure of secondary side RHR it relies on Feed and Bleed. Loss of Offsite Power caused by the reactor trip is not analysed in this section but in section 5.7 of this sub-chapter covering the LOOP event).

Loss of Residual Heat Removal fails to have a significant impact on the core damage frequency. The automatic protection systems and the availability of mitigating systems in shutdown maintain plant safety.

These accident sequences demonstrate the importance of the I&C systems for the range of primary transients from the removal of the residual heat with the safety systems, RT, LORHR, to automatic isolations, Boron Dilution, Uncontrolled Level Drop.

5.8.4. Initiating Event Analysis

5.8.4.1. Spurious Reactor Trip (RT)

5.8.4.1.1. Event Description

A spurious reactor trip corresponds to a partial or total drop of the control rods when it is not required with all parameters at their nominal value.

Following spurious RT, the control rods drop, Turbine Trip is initiated and all Main Feedwater System (ARE [MFWS]) and Startup and Shutdown System (AAD [SSS]) full-load lines are closed. The steam produced in the Steam Generators (SG) is removed to the condenser via the Main Steam Bypass. The controlled state is thus reached, defined in this case as the hot shutdown state, with residual heat being removed via the Main Steam Bypass. Feedwater supply is provided by the Main Feedwater System (ARE [MFWS]).

Note: a Loss Of Offsite Power could be caused by the Reactor Trip. This event is analysed together with LOOP as an initiating event in section 5.7 of this sub-chapter.

5.8.4.1.2. Functional Safety Requirements

The safe state is reached as follows: the Main Steam Bypass removes residual heat to the condenser and the ARE [MFWS] or AAD [SSS] systems deliver feed to the SGs.

If one of these systems fails (ARE [MFWS] or AAD [SSS]), closure of the Main Steam Isolation Valves (MSIV) is conservatively assumed. In this case the safe state is defined as the cold shutdown state with the primary circuit connected to the Residual Heat Removal System (RIS-RRA [SIS-RHRS]).

Following MSIV closure, the plant response is as described below.

- **Reactivity Control:** Reactivity control is provided by the rod drop. The consequences of a partial failure of the rod drop should be considered even in the event of a spurious Reactor Trip. This is not considered in this section but in section 5.10 of this sub-chapter on Anticipated Transient Without Scram.

- Removal of core decay heat and stored heat. This safety function is divided into:

    - **Residual heat removal:** Residual heat removal (RHR) is performed by the SGs. The steam is released first to the condenser by the main steam bypass or to the atmosphere by the VDA [MSRT] control valves. The SGs are fed either by the ARE [MFWS] system or by the AAD [SSS] system which starts automatically following a “ARE [MFWS] pumps off” signal.

      In the event of failure of the AAD [SSS] and ARE [MFWS] systems, the ASG [EFWS] system starts automatically once the “low low SG level” setpoint is reached.

      If the VDA [MSRT] valves fail to open, the Main Steam Safety Valves control the SG pressure and maintain it at about 105 bars. These valves do not support cooling the plant to the RHR connection conditions. To maintain RHR using the SGs in the long term, makeup of the ARE [MFWS] / AAD [SSS] tank or the cross-connection of the ASG [EFWS] tanks must be initiated by the operator.

      In the event of the failure of secondary side RHR, primary side RHR via Feed and Bleed is initiated by the operator. To achieve this, the Pressuriser Safety Valves or Primary Depressurisation Valves) are opened.

    - **Long term cooling:** Long term cooling is provided by the RIS [SIS] system in RHR mode.

- **Reactor Coolant System integrity:** The RCP [RCS] integrity is challenged in the event of Feed and Bleed. Feed and Bleed operation requires deliberate opening of the RCP [RCS] into the containment by the operator.

- **Reactor Coolant System inventory control:** The RCP [RCS] inventory control function is challenged by Feed and Bleed and is performed by the Medium Head Safety Injection system (MHSI).

5.8.4.1.3. Detailed Results

The Spurious Reactor Trip represents **3.2% of the Internal Event CDF with a frequency of 1.7E-08/r.y.**

The following table lists the main accident sequences. Each accident sequence corresponds to one or a group of MCS. The main accident sequences considered in the table below represent 99% of the initiating event risk.

Initiating event	***Brief description of the accident sequence***	***Frequency (per reactor per year)***
RT_A	ARE [MFWS] and AAD [SSS] fail due to total loss of digital I&C **and** the operator fails to manually control the ASG [EFWS] **and finally** the operator fails to initiate the primary Feed and Bleed or to initiate IRWST cooling with EVU [CHRS].	1.6E-08
RT_A	Main Steam Bypass fails and an I&C failure causes the failure of the VDA [MSRT] valves **and** the operator fails to initiate make-up to the tanks **and finally** the operator fails to initiate the primary Feed and Bleed.	3.6E-10
RT_A-	ARE [MFWS] and AAD [SSS] fail due to a common cause **and** ASG [EFWS] fails due to a CCF **and finally** the operator fails to initiate the primary Feed and Bleed.	8.0E-11

The following I&C system and platform are important in the protection against Spurious Reactor Trip:

- The **PS system failure**, resulting in unavailability of the ASG [EFWS] automatic control and VDA [MSRT] valves.

- The **SPPA-T2000 platform failure**, making start-up of the ARE [MFWS] and AAD [SSS] impossible.

The following operator actions are important in the protection against the Spurious Reactor Trip:

- The event “**Operator fails to start and control ASG [EFWS] with NCSS”** is important. The ASG [EFWS] is automatically started by the NCSS but not controlled. Due to the fail-safe position of the power control valve, SG feed is ensured after automatic start-up of ASG [EFWS]. Nevertheless, this is conservatively neglected in the present PSA, which increases the importance of this action.

- The event “**Operator fails to initiate primary bleed with NCSS**” is important because primary RHR provides the ultimate means of cooling in all accident sequences. For Feed and Bleed, the probability of human error is much greater than that of mechanical failure. A medium dependency is considered with the manual control of the ASG [EFWS] with NCSS.

- The event “**Operator fails to initiate IRWST cooling with EVU [CHRS] locally**” is important because EVU [CHRS] ensures IRWST cooling in total loss of digital I&C sequences where primary bleed is required.

5.8.4.2. Boron Dilution – BDIL

5.8.4.2.1. Event Description

Boron dilution initiating events are divided into two groups:

- Heterogeneous Boron Dilution:
    - The dilution is heterogeneous if unborated water slugs with a low boron concentration are formed in certain parts of the RCP [RCS], while the boron concentration in the rest of the RCP [RCS] is unchanged.
    - An unborated water slug can only form in the absence of a forced flow in the RCP [RCS]. The slug is propelled towards the core upon restarting of a Reactor Coolant Pump.
- Homogeneous Boron Dilution:
    - These are progressive events in which the boron concentration of the RCP [RCS] fluid decreases and remains homogeneous.

The initiating events are analysed in all reactor states (A to D).

5.8.4.2.2. Heterogeneous Boron Dilution

These events are characterised by the formation (and subsequent transportation into the core) of an unborated water slug of a critical size in a loop of the RCP [RCS] where homogenisation of the fluid is not guaranteed.

This could be due to an operational anomaly in a connected system, or an operator error. Subsequent flow of the slug towards and through the core could leads to local re-criticality in the core, with a potential effect on fuel integrity.

Two slug sizes have been examined:

- A 2 m^3 slug, corresponding to the largest slug which could be formed by inadvertent RCV [CVCS] injection whilst makeup is isolated, based on the use of the boron meters installed on the main RCV [CVCS] injection line.
- A 4 m^3 slug, corresponding to either the total volume in the cold leg or the volume in the loop seal, which is the maximum slug size that could be reasonably envisaged in a heterogeneous dilution scenario.

To protect against this event, the RCV [CVCS] suction line from the Volume Control Tank (VCT) is isolated following a signal generated by a safety-classified boron meter fitted downstream of the RCV [CVCS] charging pumps. This function significantly reduces the likelihood of a pure water slug being injected into the core via the RCV [CVCS] makeup line.

The suction of the RCV [CVCS] charging pumps is automatically switched over to the IRWST. In addition, measures are taken on the heat exchangers cooled by the RRI [CCWS] system and on the RCP [RCS] pumps, to prevent the formation of a pure water slug in the auxiliary systems connected via the pump seal cooling devices.

The initiating events are considered in states A and Ca (at the end of the state Ca all reactor coolant pumps are stopped). The contribution of the Heterogeneous Dilution is:

- Heterogeneous Dilution in at-power state A: 7.1E-10/r.y
- Heterogeneous Dilution in shutdown state Ca: 4.5E-09/r.y

The Heterogeneous Dilution contributes **1.0% to the Internal Event CDF** with a frequency of 5.2E-09/r.y.

5.8.4.2.3. Homogeneous Boron Dilution

With regard to Homogeneous Boron Dilution, the Volume Control Tank (VCT) and/or the REA [RBWMS] are isolatable. The dilution flow rates taken into account are:

- Dilution from the REA [RBWMS] at various flow rates, depending on the operation of the RCV [CVCS]. The following values have been derived:
    - 36 te/h in state A (1 RCV [CVCS] charging pump in operation)
    - 100 te/h in state B (2 RCV [CVCS] charging pumps in operation)
    - 72 te/h in state Ca (2 RCV [CVCS] charging pumps in operation)
    - 36 te/h in states Cb and D (1 RCV [CVCS] charging pump in operation)
- Dilution from a leak in the RRI [CCWS] heat exchanger when the system is connected to the RCV [CVCS] in operation for shutdown cooling. A leak flow of 15 te/h is assumed in states B, Ca and Cb.

At-Power state

In Power operation, the automatic control of the primary coolant temperature allows the reactivity change to be controlled by the control rods. Simultaneously, the “prevent dilution” signal initiates an automatically shut off the demineralised water supply. If this signal fails the “Anti Dilution” signal is generated leading to VCT isolation.

If the isolation fails, the reactor is tripped. Following the reactor trip, the accident sequence is the same as the one analysed below for homogeneous boron dilution in shutdown states.

Shutdown states

For a Homogeneous Dilution occurring in a shutdown state, there is an automatic isolation of the possible sources of dilution. This is achieved:

- by the Anti Dilution actuation (RPR [PS] signal) leading to VCT isolation, and
- by the Reactor Boron Water and Makeup System (REA [RBWMS]) isolation (RCSL signal).

Should isolation fail, the High Neutron Flux (source range) signal actuates the Emergency Boration System (RBS [EBS]). Subsequently, the operator must manually isolate the dilution source and shut off the demineralised water supply.

5.8.4.2.4. Functional Safety Requirements

- **Reactivity Control**:
  - **For power operation**: Following the insertion of control rods, the “prevent dilution” signal and the “Anti Dilution” signal (at-power states) isolate the dilution. Should the isolation fail, reactor trip occurs to ensure Reactivity control.

- **For shutdown (or when the reactor is tripped)**: Reactivity control is provided by isolation of the dilution following a “Anti Dilution” signal (shutdown states), by boration with the RBS [EBS] actuated following a High Neutron Flux signal and also by the manual isolation of the source of dilution.

- Removal of core decay heat and stored heat. This safety function is divided into:
  - **Residual Heat Removal**: The residual heat removal function is not challenged by the transient.
  - **Long term cooling**: Long term cooling is not challenged by the transient.

- **Reactor Coolant System integrity**: The RCP [RCS] integrity is not challenged by the transient.

- **Reactor Coolant System inventory control**: The RCP [RCS] inventory control function is not challenged by the transient.

5.8.4.2.5. Detailed Results

Homogeneous Dilution contributes **6.4% to the Internal Event CDF with a frequency of 3.4E-08/r.y.**

The following table lists the main accident sequences. Each accident sequence corresponds to one or a group of MCS. The main accident sequences considered in the table below represent 89% of the initiating event risk.

Initiating event	***Brief description of the accident sequence***	***Frequency (per reactor per year)***
DIL HO100_B-	An I&C failure causes the failure of the prevent dilution signal and of the VCT isolation due to the failure of Anti Dilution signal **and** boration fails due to failure of the RBS [EBS] (pumps or discharge line) **and** the operator fails to isolate the source of dilution.	2.2E-08
DIL HO100_B-	Total failure of digital I&C causes the failure of the VCT isolation due to the failure of Anti Dilution signal **and** the failure of RBS [EBS] actuation **and** the operator fails to isolate the source of dilution with NCSS.	4.4E-09
DIL HO--_A-	An I&C failure causes the failure of the automatic control of Average Coolant Temperature **and** the failure of VCT isolation due to the failure of Anti Dilution signal **and** the operator fails to isolate the source of dilution.	1.7E-09

Initiating event	*Brief description of the accident sequence*	*Frequency (per reactor per year)*
DIL HO100_B-	RPR [PS] failure causes the failure of the VCT isolation due to the failure of the Anti Dilution signal **and** failure of the High Neutron Flux signal, **and** failure of the High Neutron Flux alarm from NCSS due to failure of sensors or platform which prevents isolation of the source of dilution by the operator.	8.5E-10
DIL HO--_A-	I&C failures cause the failure of the automatic control of Average Coolant Temperature **and** the failure of VCT isolation due to the failure of Anti Dilution signal **and** failure of RT signals (RPR [PS] and NCSS).	7.0E-10

The following I&C signal and platform are important in the protection against the Homogenous Dilution:

- The TXS platform is important since its unavailability results in the unavailability of the prevent dilution and Anti Dilution signals necessary for the automatic isolation of the dilution and the unavailability of the automatic start of the RBS [EBS].

- The High Neutron Flux alarm from the NCSS is important because it enables the isolation of the source of dilution by the operator.

The following system is important in the protection against the Homogenous Dilution:

- The most risk significant event for the **RBS [EBS] system** is the failure of the RBS [EBS] pumps or discharge line for boration to control reactivity.

The following operator actions are important in the protection against Homogenous Dilution:

- The event "**operator fails to isolate the source of dilution**": in the event of failure of the automatic protection, the Anti Dilution signal, the operator must isolate the source of dilution.

5.8.4.3. Loss of LHSI/RHR in Shutdown States (LORHR)

5.8.4.3.1. Event Description

The initiating event considered is the loss of Low head Safety Injection in Residual Heat Removal mode (LHSI/RHR) in the shutdown states Ca, Cb and D.

The loss of RHR is defined here as the simultaneous failure of the Low Head Safety Injection (LHSI) trains which are in RHR operation. The loss of cooling chain is treated independently in sub-section 5.9 of this sub-chapter.

Note: In state E the inventory in the reactor cavity is large enough to prevent core damage for a time period longer than 24 hours without any RHR or makeup as discussed in section 4 of this sub-chapter.

The temperature of the Reactor Coolant System increases following the loss of:

- Four LHSI/RHR (state Ca),

- Three LHSI/RHR (states Cb and D), requiring activation by the operator of the LHSI standby train in RHR mode.

In State C, the return to secondary side RHR is initiated by increasing the Reactor Coolant System (RCP [RCS]) temperature to a level which enables the transfer of all decay heat to the secondary side. This is supported by the reduced set point on Main Steam Relief Valves, and only occurs if the RCP [RCS] is closed. Feed to the Steam Generators from the Emergency Feedwater System (ASG [EFWS]) is initiated automatically by the Low Steam Generator Level reactor protection (RPR [PS]) signal. The Main Steam Relief Train (VDA [MSRT]) is automatically activated following a High Steam Generator pressure reactor protection signal.

If the secondary side heat removal fails, primary RHR is initiated via feed and bleed operation in states Ca and Cb with the RCP [RCS] closed or makeup and boiling in state D with the RCP [RCS] open. For Shutdown states C and D, Medium Head Safety Injection (MHSI) is automatically actuated by two signals.

- In state Ca, a low margin to the saturation condition starts the MHSI pumps.

- In states Cb and D, low RCP-loop level starts the safety injection. Two redundant and diverse signals from the protection system and from the safety automation system are available.

For the states Cb and D, the operator has the option to start the remaining LHSI train in injection mode. The other LHSI trains are assumed lost as a consequence of the initiating event.

The operator must initiate IRWST cooling following Feed and Bleed (state C).

5.8.4.3.2. Functional Safety Requirements

Loss Of Residual Heat Removal in states Ca, Cb

- **Reactivity Control**: Reactivity control is not challenged by the transient.

- Removal of core decay heat and stored heat. This safety function is divided into:

  - **Residual Heat Removal**: In state Ca, following failure of the 4 LHSI trains in RHR mode, the residual heat removal function is provided by the secondary side RHR via the Steam Generators with their dedicated ASG [EFWS] and VDA [MSRT].

    In state Cb, following failure of the 3 LHSI trains in RHR mode, the operator must start the fourth LHSI train to perform primary side residual heat removal. As in Ca, if the fourth LHSI train fails, the RHR function is provided by the secondary side via the Steam Generators with their dedicated ASG [EFWS] and VDA [MSRT].

    In state C, if the secondary side RHR fails, primary side RHR via Feed and Bleed is initiated by the operator. RCP [RCS] bleed is provided by the Primary Depressurisation Valves or by the Pressuriser Safety Valves. RCP [RCS] feed is provided by the MHSI trains.

- **Long term cooling**: the actuation of the Feed and Bleed operation implies that residual power is transferred to the In-containment Refuelling Water Storage Tank (IRSWT). Long term cooling is provided by the cooling of the IRWST. This cooling is performed by the Containment Heat Removal System (EVU [CHRS]) and the Ultimate Cooling Water System (SRU [UCWS]).

- **Reactor Coolant System integrity**: The RCP [RCS] integrity is challenged in the event of Feed and Bleed. Feed and Bleed operation requires deliberate opening of the RCP [RCS] into the containment by the operator.

- **Reactor Coolant System inventory control**: The RCP [RCS] inventory control function is challenged during Feed and Bleed and provided by the MHSI. In state Cb, the fourth LHSI train is used for injection in addition to the MHSI.

Loss Of Residual Heat Removal in state D

- **Reactivity Control**: Reactivity control is not challenged by the transient.

- Removal of core decay heat and stored heat. This safety function is divided into:

  - **Residual Heat Removal**: Following failure of the 3 trains operating in RHR mode, the operator must start the fourth LHSI train to perform primary side residual heat removal.

    Should the primary side RHR function fail, the MHSI pumps are automatically started following the RCP [RCS] Loop level decrease. The MHSI makeup compensates for the boiling and performs the removal of the residual heat.

  - **Long term cooling**: Very long term cooling is provided by the cooling of the In-containment Refuelling Water Storage Tank (IRSWT). This cooling is performed by the Containment Heat Removal System (EVU [CHRS]) and the Ultimate Cooling Water System (SRU [UCWS]).

    Cooling of the IRWST is not required in the first 24 hours; therefore, it has not been taken into account.

- **Reactor Coolant System integrity**: In state D, the RCP [RCS] is already open.

- **Reactor Coolant System inventory control**: Control of the RCP [RCS] water inventory is provided by the automatic start-up of the MHSI trains as discussed for the RHR function. Should failure of the MHSI occur, the operator must start the remaining LHSI train in injection mode.

5.8.4.3.3. Detailed Results

The “loss of LHSI/RHR” represents **0.6% of the Internal Event CDF with a frequency of 3.2E-09/r.y.**

The following table lists the main accident sequences. Each accident sequence corresponds to one or a group of MCS. The main accident sequences considered in the table below represent 93% of the initiating event CDF.

Initiating event	*Brief description of the accident sequence*	*Frequency (per reactor per year)*
LORHR_CB	The secondary RHR fails following ASG [EFWS] and/or VDA [MSRT] failure and/or preventive maintenance on SG **and** the operator fails to start the fourth LHSI/RHR train **and** the operator fails to initiate primary Feed and Bleed.	1.6E-09
LORHR_CB	The operator fails to start the fourth LHSI/RHR train **and** the secondary RHR fails following VDA [MSRT] failure due to I&C failure **and** the operator fails to initiate primary Feed and Bleed.	6.3E-10
LORHR_D-	The operator fails to start the fourth LHSI train in RHR mode **and** the MHSI trains fail due to CCF (pumps and/or check valves) **and** the operator fails to start the fourth LHSI train in injection mode.	5.1E-10
LORHR_CA	The secondary RHR fails due to the failure of ASG [EFWS] and/or VDA [MSRT] and/or preventive maintenance on SGs **and** the operator fails to initiate primary Feed and Bleed.	1.7E-10
LORHR_CA	The secondary RHR fails following VDA [MSRT] failure due to I&C failure **and** the operator fails to initiate primary Feed and Bleed.	6.9E-11

The following I&C system and platform are important in the protection against the “Loss of LHSI/RHR”:

The most risk significant events related to **I&C systems** are failure of the TXS platform and “failure of specific logic part diversity B of the Protection System”. These two events have a relatively low probability of occurrence but their consequences are important. These events lead to the failure of the secondary RHR because of VDA [MSRT] failure in the four SGs due to failure of High SG pressure signal.

The following systems are important in the protection against the “Loss of LHSI/RHR”:

- The most risk significant event related to the **RIS [SIS] system** is the failure of the four MHSI trains. This is the back-up solution in state D if the primary side RHR function fails with the fourth LHSI train.

- **ASG [EFWS] and VDA [MSRT] systems** are important in states Ca and Cb because the residual heat removal function is provided by the secondary side.

The following operator actions are important in the protection against the “Loss of LHSI/RHR”:

- The event “**operator fails to initiate primary Feed and Bleed**”: following failure of the secondary side heat removal (states Ca and Cb), the operator must initiate Feed and Bleed.

- The event “**operator fails to start the 4th LHSI/RHR train**”: this event is present in many dominant sequences in states Cb and D because it is the first line of defence when the other three trains are lost.

5.8.4.4. Uncontrolled Level Drop (ULD)

5.8.4.4.1. Event Description

The initiating event Uncontrolled Level Drop (ULD) is defined as a failure to control the Reactor Coolant System (RCP [RCS]) level, when the level is decreased intentionally to 3/4-loop for operational purposes. This may occur in state Cb at the end of level lowering and in state D where the RCP-level is kept at 3/4-loop.

The definition and frequency of the ULD initiating events are presented in section 4 of this sub-chapter and listed above in sub-section 5.8.2 of this sub-chapter.

During an Uncontrolled Level Drop, the water level in the RCP [RCS] decreases quickly. Automatic isolation of the draining path connected to the RIS/RCV [SIS/CVCS] is implemented to avoid operational difficulties and hence any severe consequences for the core.

If the automatic isolation of the draining path fails, Medium Heat Safety Injection (MHSI) starts automatically and supports continued operation of the Residual heat removal (RHR) System. A diverse Safety Injection Signal exists in states Cb and D. The diverse signal uses diverse water level measurements. This avoids the dependency between the level measurements used for operational and safety functions.

If these actions fail, the RHR is automatically halted by the trip of the Low Head Safety Injection (LHSI) pumps when the level goes down sufficiently. Subsequently:

- In state Cb, the increase in the RCP [RCS] temperature and pressure allows the use of the secondary side for heat removal.

- In state D, manual makeup by the operator is required to compensate for boiling.

Manual isolation of the draining path is required to avoid core damage.

5.8.4.4.2. Functional Safety Requirements

ULD in shutdown state Cb

This section presents the safety functions which are challenged by the ULD event in shutdown state Cb:

- **Reactivity Control**: Reactivity control is not challenged by the transient.

- Removal of core decay heat and stored heat. This safety function is divided into:

    - **Residual Heat Removal**: Residual heat removal is provided by the Residual Heat Removal (RHR) trains in operation while the RCP [RCS] level is above the RHR trip threshold.

      The RHR function can be (re)started by the operator from the control room once the water level has been increased sufficiently to allow RHR operation.

Following RHR failure in the state Cb, the residual heat is removed by the automatic opening of the Main Steam Relief Trains (VDA) [MSRT] at their set point for cold shutdown. The steam generators are automatically fed by the Emergency Feedwater System.

Failure of heat removal via both the secondary side and the RHR System leads to core damage.

  - o **Long term cooling**: long term cooling is provided in the same way as the residual heat removal function. It is provided by either the Steam Generators or the Residual Heat Removal System.

- **Reactor Coolant System integrity**: RCP [RCS] integrity is compromised by the initiating event itself. The draining path must be isolated for the continued removal of the core decay heat.

  Automatic isolation of the draining path is provided first by the normal control (RCSL) and then by the Protection System, Safety Automation System or NCSS acting on different actuators. In the event of failure of these automatic actions, the operator must isolate the leak using the approach described in the emergency operating procedures.

  The control of the coolant inventory with safety injection discussed below gives a sufficient time window to perform manual isolation.

- **Reactor Coolant System inventory control**: following the failure of the automatic isolation, makeup is required to avoid core uncovery and to support residual heat removal.

  Makeup is either performed automatically with the MHSI pump or manually with LHSI started from the control room.

ULD in shutdown state D

This section presents the safety functions which are challenged by ULD in state D:

- **Reactivity Control**: Reactivity control is not challenged by the transient.

- Removal of core decay heat and stored heat. This safety function is divided into:

  - o **Residual Heat Removal**: Residual heat removal is provided by the Residual Heat Removal (RHR) trains in operation while the RCP [RCS] level is above the threshold for the RHR trip.

    The RHR function can be (re)started by the operator from the control room once the water level has been restored to a level sufficient for RHR operation.

    Should the RHR fail in state D, the residual heat is removed by boiling and steam discharge to the reactor building. Makeup with Safety Injection System is required to compensate for the water inventory loss and avoid core uncovery. This is discussed further under RCP [RCS] inventory below.

  - o **Long term cooling**: long term cooling is provided in the same way as the Residual Heat Removal function.

- **Reactor Coolant System integrity**: The RCP [RCS] integrity is compromised by the initiating event itself. The draining path must be isolated to maintain core decay heat removal.

  The automatic isolation of the draining path is provided first by the normal control system (RCSL) and then by the Protection System, Safety Automation System or NCSS using different actuators. In the event of failure of these automatic actions, the operator must isolate the leak using the approach described in the emergency operating procedures.

  Control of the coolant inventory with safety injection gives a sufficient time window to perform manual isolation.

- **Reactor Coolant System inventory control**: following the failure of the automatic isolation, makeup is required to avoid core uncovery, to compensate for the boiling and hence to maintain residual heat removal.

  Makeup is either performed automatically with the MHSI pump or manually with LHSI started from the control room.

5.8.4.4.3. Detailed Results for ULD

ULD represents **4.3% of the Internal Event CDF with a frequency of 2.3E-08 /r.y**.

ULD in shutdown state Cb represents 100% of the risk. The contribution of ULD to CDF in shutdown state D is negligible with a frequency of 2.4E-11 /r.y.

The following table lists the main ULD accident sequences. They represent about 89% of the risk in ULD.

Initiating event	***Brief description of the accident sequences***	***Frequency (per reactor per year)***
ULD--_CB	I&C failures (RPR [PS] level measurements) cause the uncontrolled level drop, **and**, after automatic isolation of the draining path with NCSS, automatic makeup with MHSI trains fails due to failure of RIS [SIS] signals from RPR [PS] and SAS **and** failure of the manual makeup with RIS [SIS] trains due to operator failure.	9.6E-09
ULD--_CB	I&C failures (RPR [PS] level measurements) cause the uncontrolled level drop, **and**, after automatic isolation of the draining path with NCSS, automatic makeup with MHSI trains fails due to failure of RIS [SIS] signals from RPR [PS] and SAS **and** failure of the makeup with LHSI trains due to failure to trip the RHR pumps on low low loop level from RPR [PS] and failure of the fourth LHSI train due to mechanical failure (including support systems).	8.9E-09
ULD--_CB	Failure of the automatic isolation of RCV [CVCS] and automatic makeup with MHSI trains due to the failure of main and diversified Reactor Coolant System level measurements **and** the operator fails to initiate the manual makeup with RIS [SIS] trains.	1.6E-09

The contribution of the ULD to the overall risk is reduced due to the diverse isolation and injection means available in the shutdown states.

The following systems are important in the protection against the ULD:

- The **I&C and especially the Reactor Coolant System level measurements for RPR [PS].** As described in section 4 of this sub-chapter, the reactor coolant level measurements are used by the operator to control the draining and by the protection system for the isolation of the draining path, the start of the safety injection and shutting down the RHR pumps.

  The failure of these sensors, causes the initiating event and hence the mitigation is degraded. The probability of CCF is reduced by the provision of diverse methods of level measurement.

The following operator action is important in the protection against the ULD:

- The **operator fails to start the safety injection**, in the event of failure of the MHSI, due to mechanical failure or failure of the automatic start-up signals, the operator must start Safety Injection to compensate for the leak.

5.9. LOSS OF COOLING CHAIN (LOCC)

5.9.1. Group Description

The assessment of the Loss Of the Cooling Chain (LOCC) initiating events is performed for the seven initiating events defined in section 4 of this sub-chapter.

Loss Of the Cooling Chain is defined as a partial or total loss of the Component Cooling Water System (RRI) [CCWS] or of the Essential Service Water System (SEC [ESWS]). The Loss of Ultimate Heat Sink is not included in this sub-chapter but is treated as an external event in the hazards PSA analysis presented in Sub-chapter 15.2.

The Cooling Chain is designed as follows. There are four safety classified trains corresponding to the four electrical trains and there are two headers, known as common user 1 and common user 2, and each of them can be cooled by two RRI/SEC [CCWS/ESWS] trains. In the at-power state, one train is in operation and the second is on standby. Each train of the safeguard systems is cooled by the corresponding RRI [CCWS] train independently of the header, i.e. RIS [SIS] of train 1 is cooled by train 1 of RRI [CCWS].

The following initiating events are considered in the LOCC Group:

- Leak in one common user header out of two (LOCC1 AB) leading to its unavailability.

- Leak in one operating RRI [CCWS] train out of two, but not from a common user header. The leaking train causes the automatic isolation of the common user header (LOCC2 AB). The leaking train and the corresponding common user header are assumed to be unavailable.

- Unavailability of 1 common user header out of 2 due to the failure of the operating RRI/SEC [CCWS/ESWS] train and failure of the switchover of feed to the common user header (LOCC3 AB)

- Unavailability of 1 common user header out of 2 due to failure of the operating RRI/SEC [CCWS/ESWS] train and failure of the backup train. Thus the header and its two RRI/SEC [CCWS/ESWS] trains are assumed to fail (LOCC4 AB).

- Several events correspond to a LOCC5 AB initiating event:

  - Leaks in two common user headers,

  - Leak in one common user header and leak of the operating RRI [CCWS] train which supplies the other common user header,

  - Leak in one common user header and unavailability of the other common user header due to the failure of the operating RRI/SEC [CCWS/ESWS] train and the failure of the switchover of feed to the common user header (LOCC5 AB).

  Thus the LOCC5 AB initiating event induces the unavailability of the two common user Headers and the unavailability of one out of four RRI/SEC [CCWS/ESWS] trains.

- Several events correspond to a LOCC6 AB initiating event:
  - Leak in one common user header and unavailability of the other common user header due to the failure of its two RRI/SEC [CCWS/ESWS] trains,
  - Leaks in the two operating RRI [CCWS] trains,
  - Leak in one operating RRI [CCWS] train and unavailability of the other common user header due to the failure of the operating RRI/SEC [CCWS/ESWS] train and the switchover of the common user header feed,
  - Failure of the two operating RRI/SEC [CCWS/ESWS] trains and failure of the switchover of feed to both the two common user headers.

  Thus the LOCC6 AB initiating event corresponds to the unavailability of the two common user Headers and the unavailability of two out of four RRI/SEC [CCWS/ESWS] trains.

- Several events correspond to a LOCC7 AB initiating event:
  - Leak in the operating RRI [CCWS]) train and unavailability of the other common user header due to the failure of the operating RRI/SEC [CCWS/ESWS] train and of the backup train,
  - Failure of the two operating RRI/SEC [CCWS/ESWS] trains and failure of the switchover of the feed to one common user header and failure of the backup RRI [CCWS] train to feed the other common user header,
  - Failure of the two RRI/SEC [CCWS/ESWS] operating trains and failure of the two RRI/SEC [CCWS/ESWS] backup trains

  Thus the LOCC7 AB initiating event corresponds to the unavailability of all common user Headers and to the unavailability of all RRI/SEC [CCWS/ESWS] trains.

- Failure of all RRI/SEC [CCWS/ESWS] trains in operation for residual heat removal in the shutdown states (LOCC7 Ca, LOCC7 Cb and LOCC7 D)

The definition and frequencies of the initiating events are provided in section 4 of this sub-chapter. The frequencies are tabulated in the following paragraph.

Preventive maintenance and I&C failure inducing failure of the automatic switchover of common user header feed to the RRI [CCWS] standby train are both considered in the initiating event frequency.

5.9.2. Results

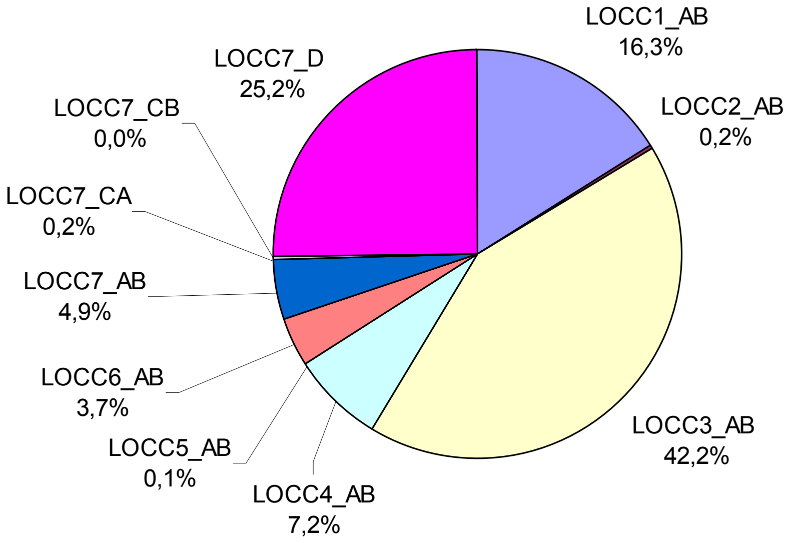
The contribution of the LOCC group to the **Internal Event Core Damage Frequency is 1.2E-07/r.y**, which represents **22.3% of the Internal Event CDF**.

The relative contribution of each LOCC initiating events within the group is given below:

Initiating Event	IE frequency (/y)	CDF (/r.y)
Partial Loss Of the Cooling Chain		
LOCC1 AB	{CCI}[a]	1.9E-08
LOCC2 AB	{CCI}[a]	2.7E-10
LOCC3 AB	{CCI}[a]	5.0E-08
LOCC4 AB	{CCI}[a]	8.5E-09
LOCC5 AB	{CCI}[a]	1.4E-10
LOCC6 AB	{CCI}[a]	4.4E-09
Total Loss of Cooling Chain		
LOCC7 AB	{CCI}[a]	5.8E-09
LOCC7 Ca	{CCI}[a]	2.6E-10
LOCC7 Cb	{CCI}[a]	1.3E-11
LOCC7 D	{CCI}[a]	3.0E-08
total		***1.2E-07***

The distribution of the risk between power and shutdown is 25% for the shutdown states (Ca, Cb and D) and 75% for the at-power states (A and B).

The contribution of each initiating event to the CDF of the LOCC group is shown in the following pie chart:



5.9.3. Dominant Accident Sequence Analysis

The following table lists the main accident sequences of the LOCC group. They represent around 98% of the overall group CDF.

Initiating event	*Brief description of the main sequence analysis*	*Frequency (per reactor per year)*
LOCC1 AB, LOCC2 AB, LOCC3 AB, LOCC4 AB, LOCC5 AB, LOCC6 AB or LOCC7 AB	The Initiating Event is followed by a LOCA as discussed in sub-section 5.9.4.1.3 below, caused by the failure to stop one Reactor Coolant Pump (I&C failure) or the failure of both RCP seals and Stand Still Seals, **and** the failure of MHSI injection due to mechanical failures of RIS [SIS] or its support systems (RRI/SEC [CCWS/ESWS]). In addition the manual actuation of Fast Secondary Cooldown fails due to I&C or operator failures.	5.6E-08
LOCC7 D	The Initiating Event is followed by the failure of the manual action (due to operator or I&C failure) to start the low head safety injection pumps cooled by their independent cooling (Safety Chilled Water System) to compensate for the boiling in the core and to avoid core uncovery.	2.5E-08
LOCC1 AB, LOCC2 AB, LOCC3 AB, LOCC4 AB, LOCC5 AB, or LOCC6 AB	The Initiating Event is followed by a LOCA as discussed in sub-section 5.9.4.1.3 below, caused by the failure to stop one Reactor Coolant Pump (I&C failure) or the failure of both RCP seals and Stand Still Seals, **and** the failure of partial cooldown due to I&C or mechanical failures. In addition the manual actuation of Feed and Bleed fails due to I&C or operator failures.	1.7E-08
LOCC1 AB, LOCC2 AB, LOCC3 AB LOCC4 AB, LOCC5 AB, LOCC6 AB or LOCC7 AB	ARE [MFWS] and AAD [SSS] fails due to total loss of digital I&C **and** the operator fails to manually control the ASG [EFWS] **and finally** failure of Feed and Bleed due to mechanical, I&C or operator failures (including failure to actuate IRWST cooling with EVU [CHRS]).	1.0E-08
LOCC7 D	The Initiating Event is followed by the mechanical failure of the Low Head Safety Injection or its support systems (e.g. Safety Chilled Water System).	4.8E-09
LOCC4 AB	The Initiating Event is followed by a seal LOCA as discussed in sub-section 5.9.4.1.3 below, caused by the failure of the Reactor Coolant Pump(s) seals and Stand Still Seals **and** the failure of the Safety Injection mainly due to failures of RRI/SEC [CCWS/ESWS] support systems. LHSI pump motor cooling with DEL [SCWS] is conservatively neglected.	3.3E-09

LOCC in power operation

Results show that the LOCC events in at-power states followed by a seal LOCA significantly contribute to the CDF of the LOCC group; they represent more than 65% of the CDF of this group. In the event of partial or total loss of the cooling chain, at least two RCP [RCS] pump motors and thermal barriers are no longer cooled. At the same time the shaft seal injection by the Chemical and Volume Control System (RCV [CVCS]) is affected. The combination of failures of the Reactor Coolant Pump shaft seals and of the Standstill Seal System (DEA [SSSS]) causes the transient to become a small LOCA.

Among the above mentioned scenarios, those which include a failure of the SPPA-T2000 platform are significant since they represent about 73% of the frequency of the overall LOCC events CDF.

LOCC in Shutdown

The total loss of the cooling chain in state D (LOCC7 D) represents approximately 25% of the CDF of this group. In this state the vessel head is removed and the water inventory is conservatively assumed to be low, at the 3/4-loop level. The residual heat removal (RHR) safety function is lost due to the failure of the RHR heat exchanger cooling by the RRI [CCWS] and the only possible mitigation is to compensate the boiling in the core by injecting cold water into the RCP [RCS]. The MHSI pumps are automatically started on a low level in the RCP [RCS] but they are unavailable because of the failure of the cooling chain. The operator must manually start the LHSI supported by a diverse cooling system, the Safety Chilled Water System (DEL [SCWS]), before the core uncovers.

It should be noted that the time window for water makeup is not based on the minimum 3/4–loop level. The time window was extended to allow a realistic evaluation whilst maintaining a sufficient level of conservatism considering that:

- The water inventory is between 3/4-loop and reactor pool flooded {CCI} [b]. The mean time window for water makeup is much greater than the one for 3/4-loop used in the thermal-hydraulic analysis.

- The safety injection signal will start the MHSI pumps even if the cooling chain is lost and they will inject a few cubic meters of water before they fail. The volume of water injected by the MHSI will increase the time window for manual LHSI start-up. This delay is not taken into account in the thermal-hydraulic analysis.

5.9.4. Initiating Event Analysis

The following items are applicable to all the initiating events of the LOCC group:

Summary of the RRI [CCWS] Design and Function

The cooling chain headers cool, amongst other components:

- The reactor coolant pump motor bearings, pump thrust bearings and thermal barriers.

- The RCV [CVCS] charging pumps.

The safety-classified part of the RRI/SEC [ESWS/CCWS] trains cools

- The RHR Heat Exchangers.
- The MHSI pump motors.
- The LHSI pump motors, but two of them may also be cooled by a diverse system, the Safety Chilled Water System (DEL [SCWS]).

It is conservatively assumed that the unavailable common header is cooling the RCV [CVCS] charging pump in operation when it fails. However the second RCV [CVCS] charging pump, cooled by the second common header, is automatically started to provide shaft seal injection to the reactor coolant pumps.

The failure of two RRI [CCWS] common headers causes the loss of reactor coolant pump motor bearings and pump thrust bearings, thermal barriers and the loss of the RCV [CVCS] charging pumps which causes the loss of shaft seal injection. Depending on the RCP [RCS] temperature and pressure, the Standstill Seal System (DEA [SSSS]) may be required to ensure the integrity of the seals when the Reactor Coolant pumps have rundown.

Because the safety-classified part of the RRI/SEC [ESWS/CCWS] trains cools the LHSI pumps and their RHR heat exchanger, the Residual Heat Removal system (RIS-RA [LHSI/RHR]) remains available even if the headers are isolated.

The impact of a Loss of Cooling Chain depends on the RCP [RCS] conditions of temperature and pressure and the means of Residual Heat Removal in operation. Therefore the initiating events will be considered separately in the at-power state and shutdown states.

Loss of Cooling Chain and Seal LOCA

Seal integrity is maintained when the seal injection by the RCV [CVCS], which is cooled by the RRI [CCWS], or the thermal barrier cooled by RRI [CCWS] are in operation. In addition, the Standstill Seal System (DEA [SSSS]) maintains Reactor Coolant System integrity when a reactor coolant pump is stopped.

A probabilistic model has been developed to address the reliability of the reactor coolant pump seals following coincident failure of seal injection and the thermal barrier. It takes into account the following parameters:

- The primary pressure and temperature.
- The initiation of the DEA [SSSS] when the pump is stopped.
- The conditional probability of failure of the DEA [SSSS] seals.
- The conditional probability of failure of the reactor coolant pump seals.

The values of both seal failure probabilities, the DEA [SSSS] and the reactor coolant pump seals, have been derived from the results of qualification tests.

5.9.4.1. Loss of Cooling Chain in Power Operation – LOCC1 AB to LOCC7 AB

As a result of the dependencies described above, the initiating event challenges the reactor coolant pump seals. If the pump is not automatically or manually stopped following the loss of cooling of the motor bearings and pump thrust bearings or the loss of seal injection and thermal barrier, the integrity of the pump is compromised. This loss of integrity causes a small LOCA in the range of 2 to 20 cm².

If the pump is tripped within the stipulated time window, the seal integrity relies on the following subsystems: the thermal barrier, lost due to the initiating event, the seal injection, affected by the initiating event, the DEA [SSSS] and the reactor coolant pump seals themselves. Failure of these barriers will cause a small LOCA in the range of 2 to 20 cm².

For these reasons two different cases have been developed for the case of loss of the cooling chain in states A and B:

- The loss of cooling chain without failure of the reactor coolant pump seals, which is **defined as a primary transient** such as Reactor Trip with multiple unavailabilities due the initiating event.

- The loss of cooling chain with the failure of the reactor coolant pump seals, which is **defined as a small LOCA** with multiple unavailabilities due to the initiating event.

5.9.4.1.1. Event Description: Loss of Cooling Chain in power operation without seal LOCAs

This section covers LOCC in at-power states **without seal LOCAs**. Due to similarity in the functional analysis, this chapter combines LOCC1 to 7 in the at-power states.

The analysis is based on the reactor trip transient described in section 5.8 of this sub-chapter.

5.9.4.1.2. Functional Safety Requirements: LOCC without Seal LOCAs.

This section presents the safety functions which are challenged by the LOCC event without seal LOCA in at-power states:

- **Reactivity Control**: Reactivity control in the transient is provided by rod drop following the reactor trip signal.

  The consequences of the failure of the rod drop are not considered in this sub-chapter. They are considered in section 5.10 of this sub-chapter discussing Anticipated Transient Without Scram.

- Removal of core decay heat and stored heat. This safety function is divided into:

  - **Residual Heat Removal**: Residual heat removal is first provided by the secondary side. The following alternatives are available:

    - To feed the SGs: Main Feedwater System (ARE [MFWS]) or the Startup and Shutdown System (AAD [SSS]) or the Emergency Feedwater System (ASG [EFWS])

- To remove steam from the SGs: Main Steam Bypass (GCT [MSB]), Main Steam Relief Valves (VDA [MSRT]) or Main Steam Safety Valves (VVP [MSSV]). The use of the Main Steam Safety Valves requires the operator to cross-connect the (ASG [EFWS]) tanks or to provide a water supply to the main feedwater (ARE [MFWS]) tank

For a partial loss of the cooling chain, LOCC1 AB, LOCC6 AB and LOCC7B AB, Feed and Bleed is claimed in the event of secondary side RHR failure.

Following a total loss of the cooling chain, LOCC7 AB, Feed and Bleed is not claimed because it requires the availability of the MHSI pumps which are cooled by the cooling chain RRI/SEC [CCWS/ESWS].

o **Long term cooling**: In the event of LOCC without seal LOCA, the long term cooling is assumed to be provided by Feed and Bleed. Cooling of the IRWST is performed by the LHSI. If cooling by the LHSI is unavailable, because of a dependency with the initiating event, cooling is provided by the Containment Heat Removal System (EVU [CHRS]).

- **Reactor Coolant System integrity**: The RCP [RCS] integrity is challenged by Feed and Bleed operation for partial loss of cooling chain. In these cases, the operator opens the Pressuriser Safety Valves or the Primary Depressurisation Valves.

- **Reactor Coolant System inventory control**: Following Feed and Bleed, safety injection (RIS [SIS]) is required and MHSI is necessary.

5.9.4.1.3. Event Description: LOCC with Seal LOCA

This section covers the LOCC in at-power states **with seal LOCAs**. Due to the similarity between the functional analyses, this chapter combines the LOCC1 AB to LOCC7 AB in the at-power states.

The analysis is based on the small Loss Of Coolant Accident discussed in section 5.1 of this sub-chapter.

5.9.4.1.4. Functional Safety Requirements: LOCC with Seal LOCAs

This section presents the safety functions which are challenged by the LOCC events with the failure of the Reactor Coolant Pumps seals:

- **Reactivity Control**: Reactivity control in the transient is provided by rod drop following the reactor trip signal.

  The consequences of failure of rod drop are not considered in this sub-chapter. They are considered in section 5.10 of this sub-chapter covering Anticipated Transients Without Scram.

- Removal of core decay heat and stored heat. This safety function is divided into:

  - **Residual Heat Removal**: Residual heat removal is provided by the secondary side. The following alternatives are available:

    - To feed the SGs: Main feedwater System (ARE [MFWS]) or the Startup and Shutdown System (AAD [SSS]) or the Emergency Feedwater System (ASG [EFWS])

    - To remove the steam from SGs: the Main Steam Relief Valves (VDA [MSRT]) or the Main Steam Safety Valves (VVP [MSSV]). In the event of the partial loss of the cooling chain, LOCC1, LOCC6 and LOCC7B, Feed and Bleed is claimed for secondary side RHR failure.

    In the event of total loss of the cooling chain LOCC7, Feed and Bleed is not claimed because it requires the availability of the MHSI pumps which are cooled by the cooling chain RRI/SEC |CCWS/ESWS].

    Note: The secondary side supports the RCP [RCS] inventory control function by depressurising the primary side using partial cooldown or fast cooldown.

  - **Long term cooling**: In the event of LOCC with seal LOCA, the long term cooling is provided by the IRWST with the LHSI pumps and RHR heat exchangers. If cooling with the LHSI is unavailable, because of a dependency with the initiating event, cooling is provided by the Containment Heat Removal System (EVU [CHRS]).

- **Reactor Coolant System integrity**: The integrity of the reactor coolant [RCS] pump seals is maintained by seal injection via the Chemical and Volume Control System (RCV [CVCS]) and the thermal barrier cooled by the Component Cooling Water System (RRI [CCWS]). When the reactor coolant pumps stop following the loss of cooling chain, the Stand Still Seal System (DEA [SSSS]) maintains the RCP [RCS] integrity with a high reliability provided the temperature and pressure remain within the design envelope.

  In the event of a LOCC with seal LOCA, the above mentioned systems have failed or the RCP [RCS] pump itself fails to stop following the loss of motor and bearing cooling due to the initiating event.

  The break size arising from the seal failure is in the lower end of small LOCA range: 2 to 20 cm².

- **Reactor Coolant System inventory control**: if the reactor coolant pump seals fail, the inventory must be controlled by the Safety Injection (RIS [SIS]).

  Prior to safety injection, the pressure in the RCP [RCS] must be decreased using the secondary side, by:

  - Automatic opening of the VDA [MSRT] or the GCT [MSB] for the partial cooldown if MHSI is available, or

  - Manual opening of the VDA [MSRT] for the fast cooldown if MHSI is unavailable.

5.9.4.1.5. Detailed Results for LOCC in at-power states (LOCC1 AB to LOCC7 AB)

The LOCC in at-power states represents about **17% of the Internal Event CDF with a frequency of 8.8E-08 /r.y**.

The LOCC with seal LOCA in power operation represents 88% of the CDF of the LOCC in at-power states.

The LOCC3 AB, failure of one operating RRI/SEC [CCWS/ESWS] train out of two followed by failure of the automatic switchover of the common user header feed to the backup RRI/SEC [CCWS/ESWS] train, contributes 57% of the CDF of the LOCC in at-power states.

The following table lists the main accident sequences of the LOCC in power operation. They represent around 98% of fault group CDF.

Initiating event	***Brief description of the main sequence analysis***	***Frequency (per reactor per year)***
LOCC1 AB, LOCC2 AB, LOCC3 AB, LOCC4 AB, LOCC5 AB, LOCC6 AB or LOCC7 AB	The Initiating Event is followed by a LOCA as discussed in sub-section 5.9.4.1.3 above, caused by the failure to stop one Reactor Coolant Pump (I&C failure) or the failure of both RCP seals and Stand Still Seals, **and** the failure of MHSI injection due to mechanical failures of RIS [SIS] or its support systems (RRI/SEC [CCWS/ESWS]). In addition the manual actuation of Fast Secondary Cooldown fails due to I&C or operator failures.	5.6E-08
LOCC1 AB, LOCC2 AB, LOCC3 AB, LOCC4 AB, LOCC5 AB, or LOCC6 AB	The Initiating Event is followed by a LOCA as discussed in sub-section 5.9.4.1.3 above, caused by the failure to stop one Reactor Coolant Pump (I&C failure) or the failure of both RCP seals and Stand Still Seals, **and** the failure of partial cooldown due to I&C or mechanical failures. In addition the manual actuation of Feed and Bleed fails due to I&C or operator failures.	1.7E-08
LOCC1 AB, LOCC2 AB, LOCC3 AB LOCC4 AB, LOCC5 AB, LOCC6 AB or LOCC7 AB	ARE [MFWS] and AAD [SSS] fail due to total loss of digital I&C **and** the operator fails to manually control the ASG [EFWS] **and finally** failure of Feed and Bleed due to mechanical, I&C or operator failures (including failure to actuate IRWST cooling with EVU [CHRS]).	1.0E-08
LOCC4 AB	The Initiating Event is followed by a seal LOCA as discussed in sub-section 5.9.4.1.3 above, caused by the failure of the Reactor Coolant Pump(s) seals and Stand Still Seals **and** the failure of the Safety Injection mainly due to failures of RRI/SEC [CCWS/ESWS] support systems. LHSI pump motor cooling with DEL [SCWS] is conservatively neglected.	3.3E-09

The following systems are important in the protection against LOCC in at-power states:

- The **Reactor Coolant Pumps**, i.e. both
  - The pump sealing system with the reactor coolant pump shaft seals, the support systems, RCV [CVCS], and the DEA [SSSS].
  - And the reactor coolant pump breakers and the associated I&C.

  The failure of one of these systems causes a small LOCA in the range 2 to 20 cm².

- The **Cooling Chain:** Essential Service Water System (SEC [ESWS]) and Component Cooling Water System (RRI [CCWS]). Part of the cooling chain may be unavailable due to the initiating event. Thus, the system becomes significant because of its reduced redundancy.

- The **I&C systems**, i.e.:
  - The SPPA-T2000 platform which may be part of the Initiating Event (switchover to standby RRI [CCWS] train), also prevents AAD [SSSS] operation and initiation of several operator actions (e.g. Fast Secondary Cooldown, Reactor Coolant Pumps trip),
  - The RPR [PS] which particularly triggers Safety Injection and control Partial Cooldown,

The following operator actions are important in protection against LOCC in at-power states:

- The **operator stops the Reactor Coolant Pumps** if the automatic trip of the pumps fails. This action is performed from the Main Control Room and the actuated breakers differ from those used by the automatic trip. Failure to trip the reactor coolant pump is assumed to lead to a small LOCA in the range 2 to 20 cm².

- The **operator starts Feed and Bleed operation.** If the secondary cooling and/or secondary depressurisation required for the partial and fast cooldown fails, the operator must initiate Feed and Bleed to remove the residual heat and perform the primary makeup.

- The **operator initiates a Fast Cooldown**. This action is required if the reactor coolant pump seals and MHSI trains fail. This action is especially significant following the total loss of the cooling chain, LOCC7 AB, because the MHSI pumps are unavailable due to the initiating event.

5.9.4.2. Total Loss Of the Cooling Chain in Shutdown States – LOCC7 Ca, Cb and D

Unlike the scenario in at-power states, the behaviour of the reactor coolant pumps seals is not an issue because the shaft seals are able to survive the RCP [RCS] pressure and temperature conditions at the cold shutdown states in the event of failure of the thermal barrier and seals injection.

Furthermore, one RIS-RA [LHSI/RHR] train is sufficient to fulfil the residual heat removal function in cold shutdown states. Consequently, only the total loss of the cooling chain is of interest in state Ca to D.

In the event of total loss of the cooling chain, LOCC 7, residual heat removal with the LHSI/RHR heat exchangers is lost and pressure and temperature rise in the reactor coolant system. The analysis is based on the following scenarios:

- The long Loss Of Offsite Power in shutdown states, LOOPL, discussed in sub-section 5.7 of this sub-chapter.
- The Loss Of Residual Heat Removal in shutdown states, LORHR, discussed in section 5.8.3 of this sub-chapter.

In the shutdown states with the RHR connected, the safety injection signal starts only the MHSI pumps. Since the MHSI motors are cooled by the cooling chain, no automatic safety injection is claimed in the states Ca, Cb and D.

5.9.4.2.1. Event Description: Total LOCC in shutdown, LOCC7 Ca, Cb and D

This section covers Total Loss Of Cooling Chain, involving unavailability of all four RRI/SEC [CWCS/ESWS] trains, in shutdown states.

5.9.4.2.2. Functional Safety Requirements: Total LOCC in shutdown, LOCC7 Ca and Cb

This section presents the safety functions which are challenged by the LOCC7 event in reactor states Ca and Cb:

- **Reactivity Control**: Reactivity control is not challenged by the transient.
- Removal of core decay heat and stored heat. This safety function is divided into:
  - o **Residual Heat Removal**: Removal of the residual heat is lost due to the failure of the Residual Heat Removal (RHR) trains in operation. The RHR trains on standby are also unavailable.

    Should the RHR fail in states Ca and Cb the residual heat is removed by the automatic opening of the VDA [MSRT] at their specific setpoint for cold shutdown. The opening of the valves will remove any steam produced in the steam generators. The Steam Generators are fed by the ASG [EFWS] trains independent from the cooling chain RRI/SEC [CCWS/ESWS].

    Failure of heat removal with the secondary side leads to a requirement for Feed and Bleed. Following a secondary side RHR failure, the operator opens the Pressuriser valves and starts makeup with the LHSI trains.

  - **Long term cooling**: Following a long term LOCC in state C, long term cooling is provided by the cooling of the IRWST following Feed and Bleed. Due to the unavailability of the cooling chain, the Containment Heat Removal System (EVU [CHRS]) is required to provide this function.

- **Reactor Coolant System integrity**: The integrity of the reactor coolant pump seals is guaranteed in shutdown state Ca. Failure to trip the reactor coolant pumps following their loss of cooling causes a RCP [RCS] leak.

  In the event of the use of Feed and Bleed, the reactor coolant system integrity is lost (State Ca and Cb).

- **Reactor Coolant System inventory control**: RCP [RCS] inventory control is challenged only in the event of Feed and Bleed in the transient. With the MHSI pumps being unavailable the operator must manually start the LHSI trains to provide makeup to the RCP [RCS].

5.9.4.2.3. Functional Safety Requirements: Total LOCC in shutdown, LOCC7 D

This section presents the safety functions which are challenged by the long LOCC event in state D:

- **Reactivity Control**: Reactivity control is not challenged by the transient.

- Removal of core decay heat and stored heat. This safety function is divided into:

  - **Residual Heat Removal**: In the event of RHR failure in state D, the residual heat cannot be removed by the steam generator as the vessel head has been removed. Makeup is performed by the Safety Injection System to compensate the boiling in the core.

  - **Long term cooling**: Flooding of the reactor cavity provides long term cooling.

- **Reactor Coolant System integrity**: RCP [RCS] integrity is not challenged by the initiating event as the RCP [RCS] is already open.

- **Reactor Coolant System inventory control**: Following the RHR failure, the water lost due to boiling must be compensated for by makeup. Automatic makeup with the MHSI trains is not possible because of the failure of the cooling chain. The operator must manually provide makeup with the LHSI pumps cooled by the Safety Chilled Water System (DEL [SCWS]).

5.9.4.2.4. Detailed Results

The total Loss Of Cooling Chain in shutdown states represents about 6**% of the Internal Event CDF** with a **core damage frequency of 3.0E-08/r.y**.

The total LOCC in state D represents more than 99% of the risk of LOCC in shutdown with a frequency of 2.99E-08/r.y.

The following table lists the main accident sequences of the LOCC in shutdown. They represent around 99% of the CDF in shutdown states.

Initiating event	*Brief description of the accident sequences*	*Frequency (per reactor per year)*
LOCC7 D	The Initiating Event is followed by the failure of the manual action (due to operator or I&C failure) to start the low head safety injection pumps cooled by their independent cooling (Safety Chilled Water System) to compensate for the boiling in the core and to avoid core uncovery.	2.5E-08
LOCC7 D	The Initiating Event is followed by the mechanical failure of the Low Head Safety Injection or its support systems (e.g. Safety Chilled Water System).	4.8E-09

As discussed in section 5.9.3 above, the Total Loss of the Cooling Chain in shutdown state D is an important contributor to the overall risk from LOCC. The main reasons were provided in the same section.

The following systems are important in the protection against Total LOCC in shutdown:

- The **Low Head Safety Injection** (Trains 1 and 4). Following a total loss of the cooling chain, safety injection is provided by LHSI trains 1 and 4 with diverse cooling means provided by the Safety Chilled Water System (DEL [SCWS]). In LOCC in state D, plant safety relies on those trains.

- The Safety **Chilled Water System** (DEL [SCWS]). The Safety Chilled Water System cools LHSI trains 1 and 4. Due to the unavailability of the cooling chain safety injection relies solely on the operation of this diverse cooling.

The following operator actions are important in the protection against Total LOCC in shutdown:

- The **operator starts LHSI cooled by the Safety Chilled Water System (DEL [SCWS])** for water makeup in state D.

5.10. ANTICIPATED TRANSIENT WITHOUT SCRAM (ATWS)

5.10.1. Group Description

The ATWS groups the events for which the required reactor trip fails because of failure of I&C signals, reactor trip actuators or mechanical blockage of control rods. These ATWS transients challenge the plant by an over-pressurisation of the primary circuit (RCP [RCS]), the core remaining critical just after the occurrence of the ATWS scenario.

The mitigation aims to protect the RCP [RCS] against the pressure peaks and injecting high boron concentration water to make the core sub-critical. Following this, the residual power must be removed.

The ATWS events studied in the PSA are:

- Total loss of main feedwater system (WS_LMF_A)
- Turbine Trip (WS_TT_A)
- Loss of main electrical network (WS_LOP_A)
- Spurious safety injection (WS_SSI_A)
- Spurious pressuriser spray (WS_PT1_A)
- Primary Breaks (WS_PB_A)
- SGTR 1 or 2 tubes (WS_SGTR_A)
- Transient of steam overflow (WS_ISF_A)

Three types of reactor trip failure are studied:

- Failure of I&C signals: For each initiating event, at least 2 redundant and diverse reactor trip signals are available. There is at least one signal actuated by the protection system (RPR [PS]) and one signal actuated by the Safety Automation System (SAS). The technology of these systems is different. Section 3.4 of this sub-chapter describes the reliability of the signals processed by the RPR and the PAS.
- Failure of reactor trip actuators: The power supply of the Control Rod Drive Mechanisms (CRDMs) can be switched off via the following features:
    - 4 main trip breakers distributed in two electrical divisions. 2 trip breakers are located in division 2, two in division 3. The main trip breakers can be opened by two coils: one with a de-energised logic (undervoltage coil), the other with an energised logic (shunt trip coil). The probability that the reactor trip fails is:

{CCI removed} a

- o 4 trip contactors combined in a 2 out of 4 logic feed a group of 4 CRDMs. Division 1 contains 11 groups of 4 CRDMs; division 4 contains 11 groups of CRDMs and 1 single CRDM for the central rod. Each trip contactor is switched off by a de-energised coil. The probability that the reactor trip fails is:

  {CCI removed} a

- o The electronics of the RodPilot can switch-off the power supply of four CRDMs. The probability that the reactor trip fails is

  {CCI removed} a

- Mechanical blockage of control rods: The number of stuck control rods that fail the reactor trip is different depending on the initiating event.

  - o Events for which the steam generator feed function is degraded lead to a less efficient heat removal by the secondary side. Thus, the primary temperature increases and the core power decreases due to the moderator feedback effect. In that case, 9 stuck control rods are sufficient to fail the reactor trip. The probability that the reactor trip fails is:

    {CCI removed} a

  - o Events for which a partial cooldown is actuated leading to a slight decrease in primary temperature. In that case, 5 stuck control rods are sufficient to fail the reactor trip. The probability that the reactor trip fails is:

    {CCI removed} a

  - o Events for which a main steam line break is postulated leading to a significant decrease in primary temperature. In that case 3 stuck control rods are sufficient to fail the reactor trip. The probability that the reactor trip fails is:

    {CCI removed} a

5.10.2. Functional Safety Requirement

- **Reactivity Control**: In the first seconds the reactivity of the core is controlled by reactivity feedbacks, dominated by the moderator effect. The ATWS analysis [Ref-1] has shown that the moderator coefficient is sufficiently negative to reduce the power production in 100% of the fuel cycle. For the pressure transient event (WS_PT1) it is unfavourable in 5% of the fuel cycle. This is based on expert judgment.

  For the remainder of the cycle, the failure of the rod drop due to actuators failure or mechanical blockage of control rods can be detected by the Protection System (RPR [PS]) which actuates a fast boration via an ATWS signal. This safety measure initiates the injection of high boron concentration water to the RCP [RCS] which takes the core sub-critical. The RBS [EBS], or the RCV [CVCS] are the two systems that provide the boration of the RCP [RCS]. The boron injected by the RCV [CVCS] is not included in the model as the charging line is isolated on high pressuriser level.

  If the RPR [PS] fails to actuate the fast boration, the diverse I&C system, the Safety Automation System (SAS) allows the operator to manually start the fast boration within 1 hour.

- **Removal of core decay heat and stored heat.** This safety function is divided into:
  - **Residual heat removal:** Residual heat removal (RHR) is provided by the SGs. The number of available systems depends on the ATWS initiating event. To simplify the event tree model it has been assumed that the steam generators are only fed by the ASG [EFWS]. This system is started automatically on “low low SG level”. The steam is released to the atmosphere via the VDA [MSRT] control valves or via the VVP [MSSV] safety valves.
  - **Long term cooling:** This function is provided by the RIS [SIS/RHR] system.
- **Reactor Coolant System integrity**: The mitigation in the first few seconds protects the RCP [RCS] against the pressure peak caused by the initiating event. The amplitude of the pressure peak, due to the increase in primary temperature, is reduced by the moderator feedback effect. The moderator effect is more efficient at controlling reactivity if the reactor coolant pumps are tripped than if they continue to operate. The reactor coolant pumps trip signal is actuated by the protection signal on the detection of an ATWS situation and low level in one steam generator.

  The overpressure protection devices available during power operation are the pressuriser safety valves (PSVs) which open automatically. One PSV is sufficient to limit the primary pressure under the design pressure if the reactor coolant pumps are tripped. If at least one reactor coolant pump is not tripped all the PSVs are conservatively required.

  The Reactor Coolant System (RCP [RCS]) integrity could be challenged by a failure of the PSV to reclose.
- **Reactor Coolant System inventory control:** If the PSVs open, the possibility that one PSV does not close should be considered. In that situation, the safety injection signal is actuated following a very low pressuriser pressure signal. This signal actuates a partial cooldown. The RCP [RCS] inventory control function has not been modelled in this case to simplify the event tree model. This is a reasonable assumption due to the very low CDF induced by this situation:
  - ATWS event, i.e. reactor trip failure, mechanical blockage of the rods, failure to reclose of one out of three PSV; the frequency of this sequence is about 7E-07/r.y. In the event of unavailability of all four MHSI trains (2.93E-04/demand), the RCP [RCS] inventory cannot be restored. This leads to core damage with a frequency of about 2E-10/r.y.

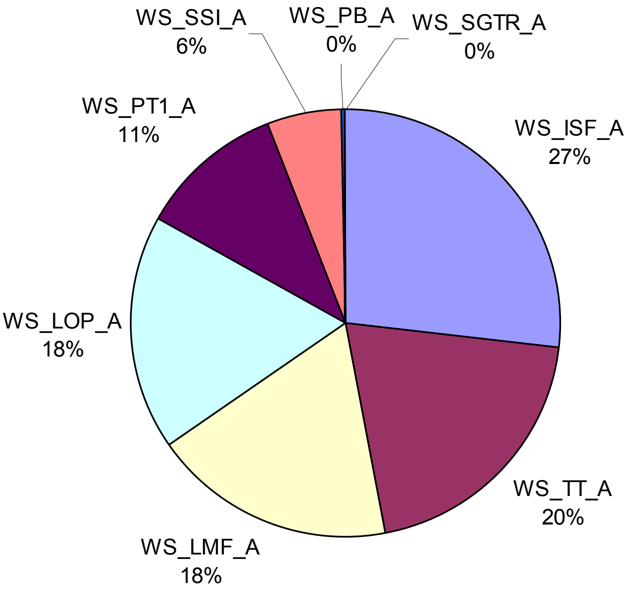
5.10.3. Results

The contribution of the ATWS group compared to the **Core Damage Frequency is 2.1E-08/r.y**. It represents **4% of the Internal Event CDF**.

The CDF for each ATWS initiating event within the group is shown in the following table:

Initiating Event	IE frequency (/y)	CDF (/r.y)
WS_ISF_A	{CCI}[a]	5.79E-09
WS_TT_A	{CCI}[a]	4.24E-09
WS_LMF_A	{CCI}[a]	3.90E-09
WS_LOP_A	{CCI}[a]	3.82E-09
WS_PT1_A	{CCI}[a]	2.38E-09
WS_SSI_A	{CCI}[a]	1.24E-09
WS_PB_A	{CCI}[a]	3.49E-11
WS_SGTR_A	{CCI}[a]	1.21E-12
total		**2.14E-08**

The relative contribution of each ATWS initiating event within the group is given below:



5.10.4. Dominant Accident Sequence Analysis

The following table lists the main accident sequences of the ATWS group. Each accident sequence corresponds to one or a group of MCS. The main accident sequences presented in the table below represent 89% of the overall group CDF.

Initiating event	***Brief description of the accident sequence***	***Frequency per reactor per year***
WS_ISF_A	The reactor trip fails because of mechanical blockage of at least 3 control rods **and** the reactivity control fails because of failure to run or start RBS [EBS]	3.6E-09
WS_TT_A	The reactor trip fails because of mechanical blockage of at least 9 control rods **and** the reactivity control fails because of failure to run or start the RBS [EBS]	3.0E-09
WS_LMF_A	The reactor trip fails because of mechanical blockage of at least 9 control rods **and** the reactivity control fails because of failure to run or start the RBS [EBS]	2.6E-09
WS_PT1_A	The reactor trip fails because of mechanical blockage of at least 5 control rods **and** the moderator coefficient is not sufficient (conservative assumption) to ensure the reactivity control at the beginning of transient	2.2E-09
WS_LOP_A	The reactor trip fails because of mechanical blockage of at least 9 control rods **and** the residual heat removal fails because of a common cause failure to run ASG [EFWS] pumps or a failure of support systems.	2.2E-09
WS_LOP_A	The reactor trip fails because of mechanical blockage of at least 9 control rods **and** the reactivity control fails because of failure to run or start the RBS [EBS]	1.2E-09
WS_ISF_A	The reactor trip fails because of mechanical blockage of at least 3 control rods **and** the residual heat removal fails because of failure to run the ASG [EFWS] pumps.	1.0E-09
WS_ISF_A	The reactor trip fails because of mechanical blockage of at least 3 control rods **and** the reactor coolant system integrity is not maintained because of common cause failure to open the pressuriser safety valves (PSVs).	9.9E-10
WS_TT_A	The reactor trip fails because of mechanical blockage of at least 9 control rods **and** the reactor coolant system integrity is not maintained because of common cause failure to open the pressuriser safety valves (PSVs).	8.4E-10
WS_SSI_A	The reactor trip fails because of mechanical blockage of at least 5 control rods **and** the reactivity control fails because of failure to run or start the RBS [EBS]	7.1E-10

Initiating event	*Brief description of the accident sequence*	*Frequency per reactor per year*
WS_LMF_A	The reactor trip fails because of mechanical blockage of 9 control rods **and** the reactor coolant system integrity is not maintained because of common cause failure to open the pressuriser safety valves (PSVs).	7.1E-10

The main contribution to the CDF is the failure of the reactivity control because of a mechanical blockage of control rods and a failure of the injection of high boron concentration water to the RCP [RCS] by the RBS [EBS].

The second main contribution to the CDF is the failure of the RCP [RCS] integrity because of a mechanical blockage of the control rods and a common cause failure to open the pressuriser safety valves (PSVs).

The third main contribution to the CDF is the failure of the secondary RHR because of a mechanical blockage of the control rods and failure of the ASG [EFWS].

For the primary pressure transient analysis the main cause of rod drop failure leading to core damage is the mechanical blockage of 5 control rods. The criterion of 5 stuck rods is used because of partial cooldown actuation on a safety injection signal. The protection systems, the RPR or the SAS are available to trip the turbine causing a heat-up of the primary circuit limited by the moderator feedback effect. Due to absence of a support study it has been assumed, supported by expert judgment, that the moderator coefficient is insufficient in 5% of cases. This assumption will be reassessed during the site licensing phase.

The following systems are important in the protection against the ATWS:

- The boration provided by the **RBS [EBS]** is important for taking the core sub-critical.
- The **Pressuriser Safety Valves (PSVs)** is important for maintaining RCP [RCS] integrity.
- The **ASG [EFWS]** is important for providing secondary RHR.

6. CONCLUSION AND INSIGHTS

This section summarises the Level 1 PSA results for internal initiating events. The PSA analyses a large range of internal initiating events in all operating modes, from the at-power state to states with the reactor core completely unloaded. The range of initiating events covered is consistent with that considered in French PSAs and with international requirements, particularly IAEA [Ref-1] and EUR requirements [Ref-2].

The consequence in terms of core damage frequency is evaluated for each initiating event enabling the assessment of the robustness of the mitigation systems provided in the EPR design.

Functional dependencies are considered between electrical power supply, cooling and I&C in the evaluation, as well as common cause failures between identical components performing the same function.

The human reliability analysis, both pre and post accident, follows the international ASEP method that considers the potential dependencies between human actions and the conditions under which the actions are performed, e.g. normal or with additional stress.

Reliability data used in the PSA are fully referenced and are consistent with French and German databases derived from extensive operating experience feedback. International databases and expert judgement are also used for some specific components.

6.1. OVERALL RESULTS

The Core Damage Frequency from internal events at power and shutdown states is 5.3E-07/r.y. This is less than the EPR probabilistic design target of 1E-06/r.y.

Section 15.1.6 - Table 1 shows the distribution of core damage frequencies between the various groups of initiating events. The distribution of the CDF between internal events is shown in Section 15.1.6 - Figure 1.

The distribution between the different plant operating states is shown in Section 15.1.6 – Figure 2. Power states A and B contribute 87% to the internal event CDF.

The time spent in the shutdown states (C to E) represents around 4% of the year and these states account for less than 13% of the internal event CDF. The distribution of risk is therefore roughly proportionate to the time ratio between power and shutdown due to the improvement in the protection during shutdown states. It should nevertheless be noted that the level of risk depends significantly on the state during shutdown. Sensitivity analysis and uncertainty analysis are presented in Sub-chapter 15.7.

6.2. SIGNIFICANT INITIATING EVENTS

As can be seen from Section 15.1.6 - Table 1 and Section 15.1.6 - Figure 1, LOCC initiating events dominate the CDF from internal events, accounting for close to 22%. The main risk consists of the potential failure to stop one Reactor Coolant Pump or failure of Reactor Coolant Pump seals (shaft seals and Stand Still Seal System) causing a small primary break following a partial or total LOCC during power operation. The second scenario highlighted by the PSA is a total loss of cooling chain in shutdown state D when the primary water inventory is low (at 3/4-loop height). In this case, the initiating event disables the RHR safety function and the automatic makeup devices. Additionally, scenarios including a dependency of the LOCC initiating events to the SPPA-T2000 I&C platform (failure of switchover to RRI [CCWS] standby train caused by I&C failure) are significant since they represent about 50% of the overall LOCC CDF.

The primary breaks contribute 20% to the Internal Event CDF with a Core Damage Frequency of 1.1E-07. In this event group, the small break in at-power states (2 – 45 cm²) contributes 5.4E-08. The significant contribution of the loss of coolant accident is mainly due to Common Cause Failures of the MHSI pumps that perform Safety Injection. The MHSI pumps are markedly less reliable than other EPR pumps.

LOOP initiating events contribute about 20% to the internal events CDF, which is mainly explained by the use of active components in the accident sequence. Furthermore SBO situations due to Common Cause Failures of the Emergency Diesel Generators or to failure of the Protection System contribute significantly to the CDF of this accident group. If consequential LOOP events following Reactor Trip are included, the contribution is increased by 8%.

Boron dilution transients, both homogeneous and heterogeneous, contribute 7% to the internal event CDF but the risk of core damage is still low at 3.9E-08/r.y. This is despite the modelling using conservative assumptions that core damage is assumed as soon as the core criticality is reached and the frequency of the initiating event is high.

ATWS initiating events contribute 4% to the internal event CDF and are mostly caused by mechanical failures. The main contribution to these sequences is the failure of the reactivity control because of a mechanical blockage of control rods, followed by failure of the RBS [EBS] pumps to inject borated water into the RCP [RCS].

Seal LOCA sequences, for which the integrity of the Main Coolant Pump seal system - SSSS, shaft seals, O-rings etc is lost, caused by LOCC events or LOOP events, including consequential LOOP, contributes 27% to the internal event CDF: 11% comes from LOCC initiating events and 16% comes from LOOP events.

The PSA analysis shows that SBO, LOOP or consequential LOOP with failure of all the EDGs contributes 8% to the internal event CDF. The main accident sequence in the case of a SBO is characterised by the failure to ensure the power supply of the plant with the LJ-Diesels (SBO diesels).

The PSA shows that the contribution of Common Cause Failures of computerised I&C platforms, either TXS or SPPA-T2000 non-specific processing parts, is highly significant, it represents 47% of the internal event CDF. The failure of the whole SPPA-T2000 platform is especially significant for the PSA results, representing 34% of the internal event CDF. Failure of the SPPA-T2000 platform induces the unavailability of most of the manual controls of the plant performed through computerised human machine interface. The low reliability value (1E-2 pfd) assigned to this I&C platform in the PSA model explains its significant contribution to the internal event CDF.

6.3. SIGNIFICANT CUTSETS AND SEQUENCES

Section 15.1.6 - Table 2 presents the 100 main minimal cutsets. These cutsets are grouped in different representative accident sequences.

The most significant cutset corresponds to the total loss of the cooling chain during shutdown state D (RCP [RCS] with vessel head off). This fault leads to the loss of the whole residual heat removal system and the automatic makeup with the medium head safety injection pumps. The initial fault is followed by the operator failure to perform make-up with the low head safety injection cooled by a diverse mean. This represents 4.5% of the internal event CDF.

The most important accident sequence corresponds to Small Loss Of Coolant Accidents (2 - 45cm²) or to Pressuriser leaks during states A and B. These faults should lead to automatic start-up of Safety Injection with MHSI, but the latter fails due to Common Cause Failure of the MHSI pumps, combined in some cases with Preventive Maintenance on one RIS [SIS] train. Additionally the manual Fast Secondary Cooldown fails to be performed in 30 minutes, either due to failure of the operator or due to I&C Human Machine Interface (HMI) failure. This group of accident sequences represents more than 10% of the internal event CDF.

SECTION 15.1.6 - TABLE 1

Distribution of core damage frequencies in initiating event group

Groups	Sub-groups	Core damage Frequency (/r.y) States A,B	Core damage Frequency (/r.y) States C,D,E	Core damage Frequency (/r.y) groups	(%)
LOCA	Loss of primary cooling Accident	1.05E-07	3.63E-09	1.08E-07	20.3%
BYPASS	LOCA leading to containment bypasses	3.70E-09	1.10E-09	4.80E-09	0.9%
RPV	Reactor Pressure Vessel Failure	1.00E-08		1.00E-08	1.9%
SSB	Breaks on secondary side (steam or water),	1.28E-08	-	1.71E-08	3.2%
	Steam line rupture with steam generator tube(s) rupture	4.32E-09	-		
SGTR	Steam generator tube (s) rupture	4.17E-09	-	4.17E-09	0.8%
Secondary Transients	Total loss of main feedwater supply	8.41E-09	-	1.79E-08	3.4%
	Loss of start-up and shutdown system	2.16E-09	-		
	Loss of Condenser	3.09E-09	-		
	Turbine Trip	4.28E-09	-		
LOOP	Total loss of offsite power (2h),	5.74E-08	2.38E-09	1.05E-07	19.8%
	Total loss of offsite power (24h),	4.30E-08	2.40E-09		
	Induced LOOP	4.23E-08	-	4.23E-08	8.0%
Primary Transients	Homogeneous boron dilution	3.29E-08	8.21E-10	8.18E-08	15.4%
	Heterogeneous boron dilution	7.05E-10	4.50E-09		
	Total loss of SIS cooling in RHR mode,	-	3.22E-09		
	Uncontrolled drop of primary level,	-	2.25E-08		
	Spurious reactor trip	1.71E-08	-		
LOCC	Partial or total loss of cooling systems,	8.84E-08	3.02E-08	1.19E-07	22.3%
ATWS	Anticipated transients without scram	2.14E-08	-	2.14E-08	4.0%
TOTAL				**5.31E-07**	100%

SECTION 15.1.6 - TABLE 2

PSA Level 1 - Main Minimal Cutsets

Group	Cutsets numbers	Group frequency	Group contribution to CDF	Cumulative Contribution to CDF	Representative Cutset	Sequence Description
1	2; 4; 5; 15; 20; 21; 36; 46; 55; 73	5.45E-08	10.27%	10.27%	Small LOCA (2-45cm²) or PZR leak - States A+B MHSI pumps CCF to run Operator fails to initiate Fast Secondary Cooldown before 30mn	Small LOCA without MHSI pumps due to a CCF to run or to start, or Preventive Maintenance on RIS [SIS], and finally failure of the operator to initiate the Fast Secondary Cooldown before 30mn to enable the LHSI to inject (operator or I&C HMI failure).
2	6; 8; 9; 76; 77; 78; 79; 90; 91; 92; 93	3.24E-08	6.10%	16.37%	Short loss of offsite power (<2h) – States A + B Combination of failures of Stand Still Seal System and Reactor Coolant Pump shaft seals Failure of non specific processing part of TXS platform (RPR [PS] failure)	Short loop with failure of automatic EDG start-up due to TXS failure, combined with failure of Reactor Coolant Pump seals. This induces a seal loss of coolant accident (no power supply for thermal barrier cooling and RCV [CVCS] seal injection). Finally failure of Partial Cooldown due to RPR [PS] unavailability.
3	1; 74	2.50E-08	4.71%	21.08%	Total loss of RRI/SEC [CCWS/ESWS] - State D Operator fails to start (through NCSS panel if SPPA-T2000 I&C platform is lost) LHSI independent of RRI/SEC [CCWS/ESWS] before 2 hours	Total loss of the cooling chain when reactor water level is at 3/4-loop height and failure of the operator to start the LHSI pumps which are not dependent on RRI/SEC [CCWS/ESWS] resulting in core uncovery.

Group	Cutsets numbers	Group frequency	Group contribution to CDF	Cumulative Contribution to CDF	Representative Cutset	Sequence Description
4	3; 14	1.55E-08	2.92%	23.99%	Spurious Reactor trip in state A	Spurious Reactor Trip followed by failure of secondary cooldown due to both I&C and operator failures. Then failure of the operator to perform Feed and Bleed (medium dependency) or to start locally EVU [CHRS] for IRWST cooling.
					Failure of non specific processing part of SPPA-T2000 platform (SAS failure)	
					Failure of non specific processing part of TXS platform (RPR [PS] failure)	
					Operator fails to start ASG [EFWS] through NCSS panel, and then fails to actuate Feed and Bleed through NCSS panel before 2 hours or fails to actuate locally EVU [CHRS] for IRWST cooling.	
5	33; 34; 58; 59; 60; 61; 96; 97	1.04E-08	1.96%	25.95%	1 RRI [CCWS] common user header unavailability – states A + B (LOCC1 and LOCC3B initiating events)	1 RRI [CCWS] common user header is unavailable due to a leak or due to a failure of the RRI [CCWS] train in operation combined with failure of the switchover to the standby train due to SPPA-T2000 failure, followed by failure of the automatic switch-over of Seal water injection by RCV [CVCS] train 2 (SPPA-T2000 platform failure). Then combination of failures of the DEA [SSSS] and of the primary pump shaft seals induces a seal LOCA. Finally CCF to run MHSI prevents the safety injection, and then the operator is not able to perform fast secondary cooldown because of the HMI unavailability (SPPA-T2000 failure).
					Failure of non specific processing part of SPPA-T2000 platform (SAS failure)	
					MHSI pumps CCF to run	
					Combination of failures of Stand Still Seal System and Reactor Coolant Pump shaft seals	

Group	Cutsets numbers	Group frequency	Group contribution to CDF	Cumulative Contribution to CDF	Representative Cutset	Sequence Description
6	7	1.00E-08	1.88%	27.83%	Failure of the Reactor Pressure Vessel	Failure of the Reactor Pressure Vessel
7	19; 25; 26; 28	9.89E-09	1.86%	29.69%	Long loss of offsite power (>2h) - States A+B	Long LOOP followed by failure of the Emergency diesel Generators due to a CCF and failure of the SBO diesels (operator failure, mechanical failure due to CCF or combination of mechanical failure and preventive maintenance) leading to the total loss of electrical supply.
					Emergency diesel generators CCF to run	
					Failure to run of the Station Blackout diesel generators or failure of their manual start-up before 2 hours	
8	38; 39; 40; 41; 42	9.29E-09	1.75%	31.44%	Uncontrolled Level Drop during state Cb	Failure of RCP [RCS] level measurements induce an uncontrolled draining of primary coolant. The decrease in water level actuates the automatic signals for water makeup with MHSI, which fails due to both sensor dependency with the initiating event and unavailability of SPPA-T2000 platform. This is followed by the failure of the operator to recover the situation through the NCSS panel.
					Failure of automatic makeup with MHSI (failure of RCP [RCS] level sensors and failure of SPPA-T2000 non specific processing part)	
					Operator fails to start LHSI for water makeup in 80 minutes through NCSS panel	

Group	Cutsets numbers	Group frequency	Group contribution to CDF	Cumulative Contribution to CDF	Representative Cutset	Sequence Description
9	10; 32; 45	9.10E-09	1.71%	33.16%	1 RRI [CCWS] common user header unavailability – states A + B (LOCC1 and LOCC3B initiating events)	1 RRI [CCWS] common user header is unavailable due to a leak or due to a failure of the RRI [CCWS] train in operation combined with failure of the switchover to the standby train due to SPPA-T2000 failure. No seal LOCA occurs. Then secondary cooldown fails due to both I&C and operator failures. Then failure of the operator to perform Feed and Bleed (medium dependency) or to start locally EVU [CHRS] for IRWST cooling.
					Failure of non specific processing part of SPPA-T2000 platform (SAS failure)	
					Failure of non specific processing part of TXS platform (RPR [PS] failure)	
					Operator fails to start and control ASG [EFWS] for secondary cooldown through NCSS panel, and then fails to initiate Feed and Bleed before 2 hours through NCSS panel or fails to start locally EVU [CHRS] for IRWST cooling	
10	18; 47; 70; 94; 95	7.06E-09	1.33%	34.49%	Secondary transient – states A + B	Secondary transient (Turbine Trip, Loss of Condenser, Loss of Main Feedwater) followed by failure of secondary cooldown due to both I&C and operator failures. Then failure of the operator to perform Feed and Bleed (medium dependency). or to start locally EVU [CHRS] for IRWST cooling.
					Failure of non specific processing part of SPPA-T2000 platform (SAS failure)	
					Failure of non specific processing part of TXS platform (RPR [PS] failure)	
					Operator fails to start and control ASG [EFWS] for secondary cooldown through NCSS panel, and then fails to initiate Feed and Bleed in 2 hours through NCSS panel or fails to start locally EVU [CHRS] for IRWST cooling	

Group	Cutsets numbers	Group frequency	Group contribution to CDF	Cumulative Contribution to CDF	Representative Cutset	Sequence Description
11	30; 31; 52; 53	6.91E-09	1.30%	35.79%	Small LOCA (2-45cm²) + PZR leak - States A+B Failure of specific logic part PS diversity B or of TXS non specific processing part (RPR [PS] failure) Failure of GCT [MSB] Operator fails to actuate the partial cooldown in 15mn Operator fails to initiate Feed and Bleed operation in 30mn	Small LOCA with VDA [MSRTs] unavailable due to I&C failure and neither recovered by GCT [MSB] nor by the operator in 15mn. Partial cooldown is therefore not performed, thus the LHSI/MHSI cannot inject into the RCP [RCS]. Finally failure of the operator to perform Feed & Bleed (medium dependency).
12	37; 49; 50; 51	6.60E-09	1.24%	37.03%	Spurious reactor trip in state A Consequential Long loss of offsite power (>2h) Emergency diesel generators CCF to run Failure to run of the Station Blackout diesel generators or failure of their manual start-up before 2 hours	The spurious reactor trip induces a long LOOP, then the event is followed by typical LOOP sequences (see group 7)

Group	Cutsets numbers	Group frequency	Group contribution to CDF	Cumulative Contribution to CDF	Representative Cutset	Sequence Description
13	57; 62; 63; 66; 75; 80	6.42E-09	1.21%	38.24%	ATWS - Excessive Steam flow, Turbine Trip or Loss of Main Feedwater - State A	ATWS: # Excessive Steam flow with failure of reactor trip due to mechanical blockage of at least 3 out of 89 control rods, # or Turbine Trip or Loss of Main Feedwater due to mechanical blockage of at least 9 out of 89 control rods, and core damage because of mechanical failure of boration with RBS [EBS] due to a CCF.
					At least 3 out of 89 rods stuck for Excessive Steam Flow, at least 9 out of 89 rods stuck for Turbine Trip and Loss of Main Feedwater	
					RBS [EBS] pumps CCF to run	
14	81; 82; 83; 84; 85; 86; 87; 88	6.32E-09	1.19%	39.43%	Homogeneous boron dilution via REA [RBWMS], dilution around 100 t/h - State B	Homogeneous boron dilution followed by failure of TXS (PS and RCSL) anti-dilution signals, RBS [EBS] failure and no manual isolation of the source of dilution in 25mn.
					Failure of specific logic part PS diversity B or of TXS non specific processing part (RPR [PS] failure)	
					RBS [EBS] pump failure to run or to start	
					Manual dilution isolation failure before 25 mn	
15	11; 56	5.86E-09	1.10%	40.53%	Small Secondary Steam Break upstream MSIV - States A+B	Small secondary side break upstream MSIV followed by isolation of MSIV. Overcooling of the affected SG due to failure (operator or I&C failure) to stop the ASG [EFWS] injection in this SG, and failure of the MHSI pumps to start boration of the RCP [RCS].
					MHSI pumps CCF to run	
					Failure of the manual stop of ASG [EFWS] of the blow down SG (operator or I&C HMI failure)	

Group	Cutsets numbers	Group frequency	Group contribution to CDF	Cumulative Contribution to CDF	Representative Cutset	Sequence Description
16	17; 27	5.63E-09	1.06%	41.59%	Long loss of offsite power (>2h) - States A+B (including consequential long LOOP after spurious Reactor Trip in state A) Emergency diesel generators CCF to run Mechanical failure of the Reactor Coolant pumps shaft seals Failure of the operator to perform RCP [RCS] cooling by cross connecting SGs (local to plant action) and opening MSRT	Long LOOP followed by a SBO situation due to CCF to run the Emergency diesel generators. Then seal LOCA occurs due to both mechanical failure of the primary pumps shaft seals, and failure of the operator to perform manually RCP [RCS] cooldown to ensure correct operation of the Stand Still Seal System. Finally failure of the operator to manually perform Fast Secondary Cooldown (total dependency with the manual action of primary cooldown).
17	12; 98	5.21E-09	0.98%	42.57%	Heterogeneous boron dilution - States A or Ca	Heterogeneous boron dilution during states Ca or A leading directly to core damage.
18	22; 23	5.11E-09	0.96%	43.53%	Short loss of offsite power (<2h) - States A+B Failure of specific logic part PS diversity A or of TXS non specific processing part (PS failure) Operator fails to start and control ASG [EFWS] for secondary cooldown, and then fails to initiate Feed and Bleed in 2 hours.	Short LOOP followed by failure of secondary cooldown due to both I&C PS failure and failure of the operator to start and control ASG [EFWS]. Then the operator fails to perform Feed and Bleed (medium dependency).

Group	Cutsets numbers	Group frequency	Group contribution to CDF	Cumulative Contribution to CDF	Representative Cutset	Sequence Description
19	13	4.38E-09	0.82%	44.36%	Homogeneous boron dilution via REA [RBWMS], dilution around 100 t/h - State B	Homogeneous boron dilution during state B followed by failure of both RCSL and RPR [PS] automatic antidilution signals, and failure of the manual start-up of boration due to unavailability of the HMIs (SPPA-T2000 and TXS platforms). Finally the operator fails to isolate dilution before 25 min through the NCSS panel.
					Failure of non specific processing part of SPPA-T2000 platform (SAS failure)	
					Failure of non specific processing part of TXS platform (RPR [PS] failure)	
					Operator fails to isolate the dilution in 25 min through NCSS panel	
20	16	3.70E-09	0.70%	45.05%	V-LOCA during power states AB	V-LOCA during power or hot standby states, conservatively assumed to lead directly to core damage.
21	43; 44	3.65E-09	0.69%	45.74%	Medium Break LOCA (100-180cm2) – States A + B	Medium Break LOCA followed by failure of the Safety Injection due to CCF to run MHSI pumps.
					MHSI pumps CCF to run	

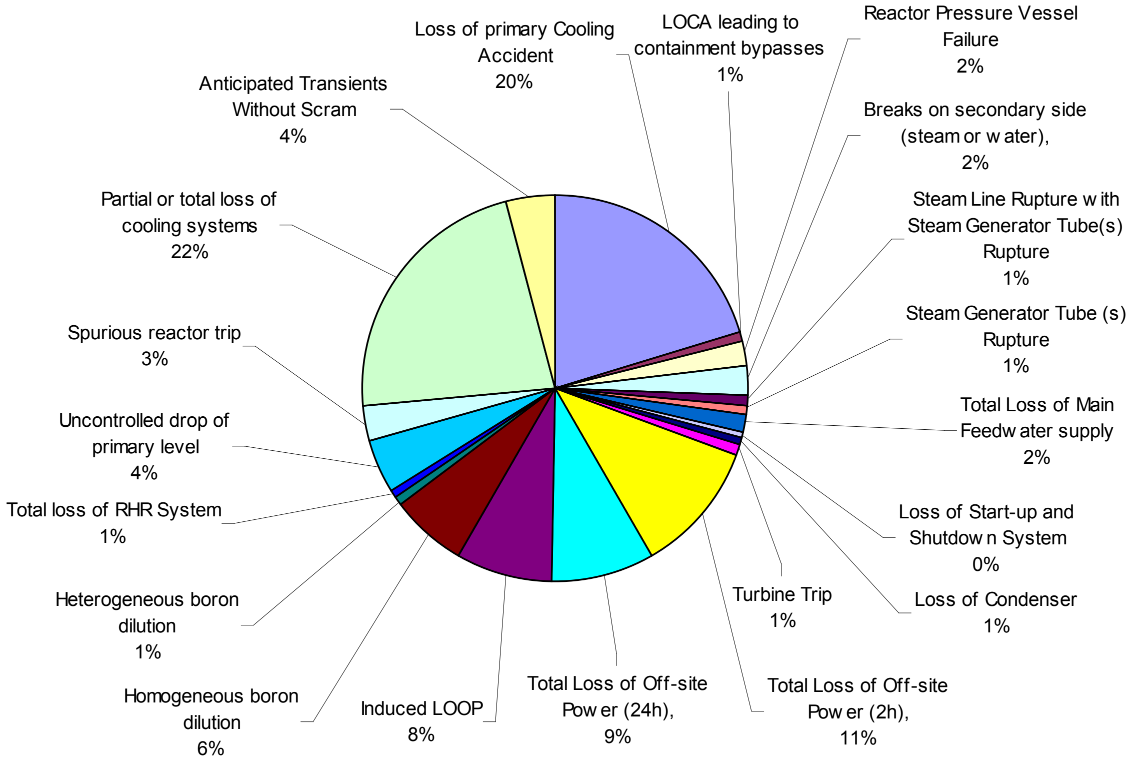
Group	Cutsets numbers	Group frequency	Group contribution to CDF	Cumulative Contribution to CDF	Representative Cutset	Sequence Description
22	24; 89	3.32E-09	0.62%	46.37%	Loss of Main Feedwater – State A	Loss of Main Feedwater followed by failure of secondary cooldown due failure of both AAD [SSS] and ASG [EFWS] systems, and failure of the operator to perform manual Feed and Bleed.
					Mechanical failure of the Start-up and Shutdown System	
					ASG [EFWS] pumps CCF to run	
					Operator fails to perform Feed and Bleed in 2 hours	
23	29	2.16E-09	0.41%	46.77%	ATWS - Spurious pressuriser spray - State A	ATWS: Spurious pressuriser spray with failure of reactor trip due to mechanical blockage of at least 5 out of 89 control rods and core damage because of an assumed unfavourable moderator feedback coefficient.
					At least 5 out of 89 rods stuck	
					Unfavourable moderator coefficient	
24	64; 65	2.10E-09	0.40%	47.17%	1 RRI [CCWS] common user header unavailability – states A + B (LOCC3B initiating events)	Failure of the operating RRI [CCWS] train and of the switchover to standby train (SPPA-T2000 failure) leading to unavailability of one common user header out of two. Unavailability of both SPPA-T2000 and NCSS platforms causes a failure to trip the primary pumps, and therefore a small LOCA. Then failure of Safety injection with MHSI due to a CCF, and finally failure of manual Fast Secondary Cooldown actuation due to HMI failure (SPPA-T2000 failure).
					Failure of non specific processing part of SPPA-T2000 platform (SAS failure)	
					Failure of the whole NCSS I&C platform	
					MHSI pumps CCF to run	

Group	Cutsets numbers	Group frequency	Group contribution to CDF	Cumulative Contribution to CDF	Representative Cutset	Sequence Description
25	67; 69	2.00E-09	0.38%	47.55%	Large Secondary Break downstream MSIV - States A+B Failure of non specific processing part of SPPA-T2000 platform (SAS failure) Failure of specific logic part PS diversity B or of TXS non specific processing part (RPR [PS] failure)	Large Secondary Break downstream MSIV followed by a failure to close the four MSIVs, due to I&C failures (RPR [PS] diversity B and SPPA-T2000). Then failure of automatic actuation of safety injection by MHSI, due to I&C failures.
26	71; 72	1.92E-09	0.36%	47.91%	Medium Break LOCA (45-100cm2) – States A + B MHSI pumps CCF to run Operator fails to initiate Fast Secondary Cooldown before 15mn	Medium break LOCA followed by failure of automatic safety injection due to MHSI CCF to run, and then failure of the operator to perform Fast Secondary Cooldown to enable the LHSI to inject.

Note: the cutsets #35, #48, #54, #68, #99 and #100 are not listed in this table. They contribute to 7.38E-09..

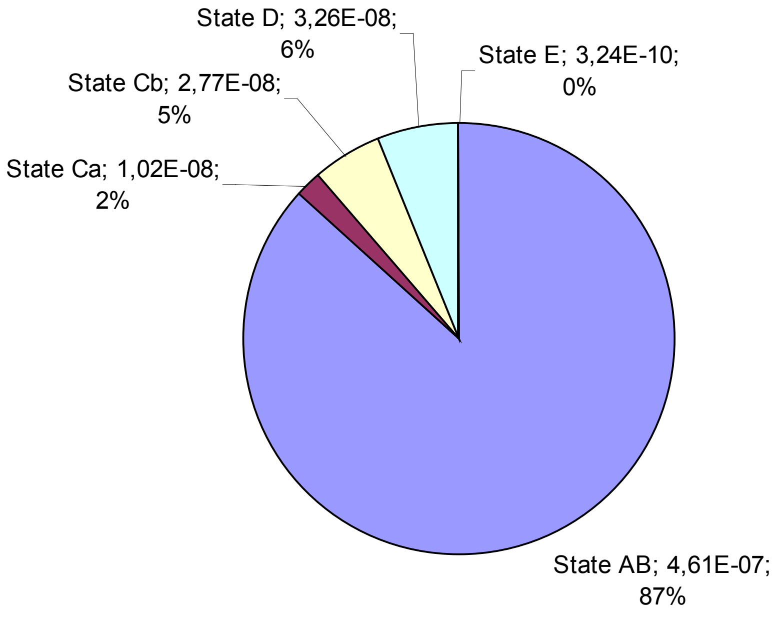
SECTION 15.1.6 - FIGURE 1

Distribution of core damage frequencies per initiating event group



SECTION 15.1.6 - FIGURE 2

Distribution between the different plant operating states



SUB-CHAPTER 15.1 - REFERENCES

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

1. INTRODUCTION

[Ref-1] RELCON SCANDPOWER AB. “RiskSpectrum® PSA Professional 2.10, Quality Manual, Test protocols and Release Approval”. 2006. (E)

3. METHODOLOGY

3.1. PLANT OPERATING STATES

3.1.2. Scope

[Ref-1] EPR Basic Design Report. Issue February 1999. (E)

3.2. RELIABILITY DATA

[Ref-1] H. Gentner. Summary of the input data for UK EPR Probabilistic Safety Assessment NEPS-F DC 565 Revision A FIN. AREVA. May 2010. (E)

[Ref-2] Centralised Reliability and Events Database (ZEDB) – Reliability Data for Nuclear Power Plant Components – Analysis for 2004.
Report VGB-TW804e. VGB PowerTech Service GmbH. ISSN 1439-7498. (E)

[Ref-3] Centralised Reliability and Events Database (ZEDB) – Reliability Data for Nuclear Power Plant Components – December 2006.
Report VGB-TW805. VGB PowerTech Service GmbH. ISSN 1439-7498. (E)

[Ref-4] S.A. Eide, S.V. Chmielewski, and T.D. Swantz. EG&G - Generic Component Failure Data Base for Light Water and Liquid Sodium Reactor PRAs. EG&G Idaho Inc., Idaho National Laboratory.
EGG-SSRE-8875. February 1990. (E)

3.3. COMMON CAUSE FAILURES

[Ref-1] European Utility Requirements for LWR Nuclear Power Plants, Volume 2: Generic Nuclear Island Requirements, Chapter 17: PSA Methodology, Revision B.
EUR Document. November 1995. (E)

3.4. INSTRUMENTATION AND CONTROL

3.4.1. Methodology

3.4.1.1. Instrumentation part

[Ref-1] C. Leroy. UK EPR : Description of the C&I modelling in the PSA NEPS-F DC 576 Revision A FIN. AREVA. July 2010. (E)

3.4.1.5.1. Modelling of the Human Machine Interface

[Ref-1] C. Leroy. UK EPR : Description of the C&I modelling in the PSA NEPS-F DC 576 Revision A FIN. AREVA. July 2010. (E)

3.4.1.5.2. Modelling of Non Computerised Safety System

[Ref-1] C. Leroy. UK EPR : Description of the C&I modelling in the PSA NEPS-F DC 576 Revision A FIN. AREVA. July 2010. (E)

3.4.2. Instrumentation and control unavailability values

3.4.2.1. Instrumentation part

[Ref-1] C. Leroy. UK EPR : Description of the C&I modelling in the PSA NEPS-F DC 576 Revision A FIN. AREVA. July 2010. (E)

3.4.3. Integration of Instrumentation and Control system in the PSA model

3.4.3.2. PSA modelling assumptions

[Ref-1] F. Godefroy. Human Reliability Analysis Notebook of the UK EPR Probabilistic Safety Assessment. NEPS-F DC 191 Revision A FIN. AREVA. January 2010. (E)

[Ref-2] C. Leroy. UK EPR : Description of the C&I modelling in the PSA NEPS-F DC 576 Revision A FIN. AREVA. July 2010. (E)

3.5. HUMAN RELIABILITY ANALYSIS

[Ref-1] F Godefroy. Human Reliability Analysis Notebook of the UK EPR Probabilistic Safety Assessment. NEPS-F DC 191 Revision A. AREVA. January 2010. (E)

[Ref-2] A D Swain. Accident Sequence Evaluation Program Human Reliability Analysis Procedure.
NUREG/CR-4772. Sandia National Laboratories, Albuquerque, New Mexico. February 1987. (E)

3.5.2. Post-Accident Tasks

3.5.2.1. Diagnosis Model

[Ref-1] A D Swain. Accident Sequence Evaluation Program Human Reliability Analysis Procedure.
NUREG/CR-4772. Sandia National Laboratories, Albuquerque, New Mexico. February 1987. (E)

3.5.2.2. Time dependency between diagnosis and post-diagnosis actions

[Ref-1] F Godefroy. Human Reliability Analysis Notebook of the UK EPR Probabilistic Safety Assessment. NEPS-F DC 191 Revision A. AREVA. January 2010. (E)

[Ref-2] System Design Manual - Emergency Feedwater System (EFWS), Part 2 – System Operation. SFL-EFMF-2006.829 Revision E1. SOFINEL. September 2009. (E)

3.5.2.4. Screening of post-accident human actions

[Ref-1] EPR Basic Design Report. Issue February 1999. (E)

3.6. SYSTEM MODELLING

3.6.2. System Mission Time

[Ref-1] A. Drevet. OL3 PSA Support Studies. NEPR-F DC 241 Revision B FIN. AREVA/SIEMENS. June 2008. (E)

3.6.3. Support Systems

[Ref-1] UK EPR. Probabilistic Safety Analysis Level 1 Detailed Documentation. NEPS-F DC 355 Revision C FIN. AREVA. June 2010. (E)

3.7. ACCIDENT SEQUENCE ANALYSIS

3.7.2. Consequences

[Ref-1] A. Drevet. OL3 PSA Support Studies. NEPR-F DC 241 Revision B FIN. AREVA/SIEMENS. June 2008. (E)

SECTION 15.1.3 - TABLE 1

[Ref-1] H. Gentner. Summary of the input data for UK EPR Probabilistic Safety Assessment NEPS-F DC 565 Revision A FIN. AREVA. May 2010. (E)

SECTION 15.1.3 - TABLE 2

[Ref-1] H. Gentner. Summary of the input data for UK EPR Probabilistic Safety Assessment NEPS-F DC 565 Revision A FIN. AREVA. May 2010. (E)

[Ref-2] S.A. Eide, S.V. Chmielewski, and T.D. Swantz. EG&G - Generic Component Failure Data Base for Light Water and Liquid Sodium Reactor PRAs. EG&G Idaho Inc., Idaho National Laboratory.
EGG-SSRE-8875. February 1990. (E)

[Ref-3] Centralised Reliability and Events Database (ZEDB) – Reliability Data for Nuclear Power Plant Components – Analysis for 2004.
Report VGB-TW804e. VGB PowerTech Service GmbH. ISSN 1439-7498. (E)

[Ref-4] Centralised Reliability and Events Database (ZEDB) – Reliability Data for Nuclear Power Plant Components – December 2006.
Report VGB-TW805. VGB PowerTech Service GmbH. ISSN 1439-7498. (E)

SECTION 15.1.3 - TABLE 3

[Ref-1] C. Leroy. UK EPR : Description of the C&I modelling in the PSA
NEPS-F DC 576 Revision A FIN. AREVA. July 2010. (E)

SECTION 15.1.3 - TABLE 4

[Ref-1] A D Swain. Accident Sequence Evaluation Program Human Reliability Analysis Procedure.
NUREG/CR-4772. Sandia National Laboratories, Albuquerque, New Mexico. February 1987. (E)

4. INTERNAL INITIATING EVENTS

4.1. SCOPE

[Ref-1] S. Kahia. Analysis of the Completeness of Scope of Initiating Events for the GDA Step 3 UK Probabilistic Safety Assessment. NEPS-F DC 377 Revision B. AREVA. December 2009. (E)

[Ref-2] Defining Initiating Events for Purposes of Probabilistic Safety Assessment.
IAEA-TECDOC-719. Vienna. IAEA. 1993. (E)

[Ref-3] V. Sorel. EPR PSA Assessment of initiating event frequencies.
ENFPFC0200484. Revision A. EDF. February 2003. (E)

[Ref-4] EPR Basic Design Report. Issue February 1999. (E)

[Ref-5] Probabilistic Safety Assessment of reactor unit 3 in the Paluel Nuclear Power Center (1300MWe), Overall Report.
EDF. May 1990. (E)

[Ref-6] Études probabiliste de sureté des réacteurs à eau sous pression de 900 MWe, Rapport de synthèse.
[Probabilistic Safety Assessment of 900 MWe (French) Pressurised Water Reactors].
IPSN. April 1990.

[Ref-7] Development of Transient Initiating Event Frequencies for Use in Probabilistic Risk Assessment.
NUREG/CR-3862. NRC. May 1985. (E)

[Ref-8] Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants.
NUREG/CR-6928. NRC. February 2007. (E)

[Ref-9] Estimating Loss-of-Coolant Accident (LOCA) Frequencies through the Elicitation Process.
NUREG-1829. NRC. April 2008. (E)

[Ref-10] EDF. FA3 EPR - Preliminary Safety Analysis Report, Chapter 18.1 “Probabilistic Safety Analysis – level 1”. 2006. (E)

4.1.3. Quantification of the frequency of initiating events

[Ref-1] Development of Transient Initiating Event Frequencies for Use in Probabilistic Risk Assessment.
NUREG/CR-3862. NRC. May 1985. (E)

[Ref-2] Defining Initiating Events for Purposes of Probabilistic Safety Assessment.
IAEA-TECDOC-719”. Vienna. IAEA. 1993. (E)

[Ref-3] V. Sorel. EPR PSA Assessment of initiating event frequencies.
ENFPFC0200484. Revision A. EDF. February 2003. (E)

[Ref-4] Probabilistic Safety Assessment of reactor unit 3 in the Paluel Nuclear Power Center (1300MWe), Overall Report.
EDF. May 1990. (E)

[Ref-5] Études probabiliste de sureté des réacteurs à eau sous pression de 900 MWe, Rapport de synthèse.
[Probabilistic Safety Assessment of 900 MWe (French) Pressurised Water Reactors.]
IPSN. April 1990.

[Ref-6] H. Gentner. Summary of the input data for UK EPR Probabilistic Safety Assessment
NEPS-F DC 565 Revision A FIN. AREVA. May 2010. (E)

4.2. LOSS OF PRIMARY COOLANT ACCIDENTS (LOCA)

4.2.1. Primary breaks

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

[Ref-2] Estimating Loss-of-Coolant Accident (LOCA) Frequencies through the Elicitation Process.
NUREG-1829. NRC. April 2008. (E)

[Ref-3] Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants.
NUREG/CR-6928. NRC. February 2007. (E)

[Ref-4] V. Roux. EPR - Reliability Study of the FA3 SEMPELL Pressurizer Safety Relief Valves.
NEPS-F DC 109 Revision C. AREVA. October 2007. (E)

4.2.2. Reactor Pressure Vessel Failure

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

4.2.3. Interfacing system LOCA (V-LOCA)

[Ref-1] F. Satin. EPR – Probabilistic Analysis of Accident Sequences Caused by Interfacing Loss of Coolant Accidents.
EPSE DC 833 Revision F. AREVA. March 2006. (E)

[Ref-2] Der Bundesminister für Forschung und Technologie (BMFT) (Hrsg.): Deutsche Risikostudie Kernkraftwerke, Phase B. Verlag TÜV Rheinland GmbH. Köln. 1990.
[Minister of Research and Technology: German Safety Analysis of Nuclear Power Plants, Phase B. Publisher TÜV Rheinland GmbH. Cologne. 1990.]

4.2.4. Steam Generator Tube(s) Rupture (SGTR)

[Ref-1] V. Sorel. EPR PSA Assessment of initiating event frequencies.
ENFPFC0200484. Revision A. EDF. February 2003. (E)

4.3. SECONDARY SYSTEM BREAKS (SLB)

4.3.1. Breaks on Secondary System (steam or feed water)

[Ref-1] Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants.
NUREG/CR-6928. NRC. February 2007. (E)

[Ref-2] V. Sorel. EPR PSA Assessment of initiating event frequencies.
ENFPFC0200484. Revision A. EDF. February 2003. (E)

4.3.2. Secondary Breaks and SGTR

[Ref-1] V. Sorel. EPR PSA Assessment of initiating event frequencies.
ENFPFC0200484. Revision A. EDF. February 2003. (E)

[Ref-2] Steam Generator Tube Failure.
NUREG/CR-6365. NRC and Idaho National Engineering Laboratory. April 1996. (E)

4.4. SECONDARY SYSTEM TRANSIENTS

4.4.3. Spurious Turbine Trip (TT_A)

[Ref-1] V. Sorel. EPR PSA Assessment of initiating event frequencies.
ENFPFC0200484. Revision A. EDF. February 2003. (E)

4.4.4. Loss of condenser (LOC_AB)

[Ref-1] European Utility Requirements for LWR Nuclear Power Plants, Volume 2: Generic Nuclear Island Requirements, Chapter 17: PSA Methodology, Revision B.
EUR Document. November 1995. (E)

4.5. LOSS OF ELECTRICAL SUPPLY

4.5.1. LOOP during Power Operation (states A and B)

[Ref-1] European Utility Requirements for LWR Nuclear Power Plants, Volume 2: Generic Nuclear Island Requirements, Chapter 17: PSA Methodology, Revision B.
EUR Document. November 1995. (E)

[Ref-2] V. Sorel. EPR PSA Assessment of initiating event frequencies.
ENFPFC0200484. Revision A. EDF. February 2003. (E)

4.5.2. LOOP during shutdown states (states Ca, Cb, D and E)

[Ref-1] European Utility Requirements for LWR Nuclear Power Plants, Volume 2: Generic Nuclear Island Requirements, Chapter 17: PSA Methodology, Revision B.
EUR Document. November 1995. (E)

4.5.3. Consequential LOOP

[Ref-1] A Reassessment of the Frequency and Duration of Loss of Off-Site Power.
SXB-IP-096233. April 1991. (E)
(This document is a National Grid Report: NGD/SD/4/89. August 1990.)

[Ref-2] Re-evaluation of Station Blackout Risk at Nuclear Power Plants, Analysis of Loss of Offsite Power Events: 1986 – 2004. NUREG/CR-6890 Volume 1.
December 2005. (E)

4.6. PRIMARY TRANSIENTS

4.6.2. Boron Dilution (BDIL)

[Ref-1] Heterogeneous Boron Dilution - PSA demonstration of dilution accident practical elimination.
NGPS4/2003/en/0120 Revision B. TR 04/138. AREVA. December 2003. (E)

4.6.2.1. Heterogeneous Boron Dilution

[Ref-1] Heterogeneous Boron Dilution - PSA demonstration of dilution accident practical elimination.
NGPS4/2003/en/0120 Revision B. TR 04/138. AREVA. December 2003. (E)

4.6.2.2. Homogeneous Boron Dilution

[Ref-1] V. Sorel. EPR PSA Assessment of initiating event frequencies.
ENFPFC0200484. Revision A. EDF. February 2003. (E)

4.8. ANTICIPATED TRANSIENTS WITHOUT SCRAM (ATWS)

[Ref-1] C. Duval. EPR – Probabilistic Analysis of Accident Sequences Caused by Anticipated Transients Without Scram.
PSSE DC 901 Revision C. AREVA. October 2004. (E)

SECTION 15.1.4 - TABLE 1

[Ref-1] F. Satin. EPR – Probabilistic Analysis of Accident Sequences Caused by Interfacing Loss of coolant Accidents.
EPSE DC 833 Revision F. AREVA. March 2006. (E)

SECTION 15.1.4 - TABLE 2

[Ref-1] V. Sorel. EPR PSA Assessment of initiating event frequencies.
ENFPFC0200484. Revision A. EDF. February 2003. (E)

[Ref-2] European Utility Requirements for LWR Nuclear Power Plants, Volume 2: Generic Nuclear Island Requirements, Chapter 17: PSA Methodology, Revision B.
EUR Document. November 1995. (E)

[Ref-3] Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants.
NUREG/CR-6928. NRC. February 2007. (E)

[Ref-4] Estimating Loss-of-Coolant Accident (LOCA) Frequencies through the Elicitation Process.
NUREG-1829. NRC. April 2008. (E)

[Ref-5] V. Roux. EPR - Reliability Study of the FA3 SEMPELL Pressurizer Safety Relief Valves,
NEPS-F DC 109 Revision C. AREVA. October 2007. (E)

SECTION 15.1.4 - TABLE 3

[Ref-1] Heterogeneous Boron Dilution - PSA demonstration of dilution accident practical elimination.
NGPS4/2003/en/0120 Revision B. TR 04/138. AREVA. December 2003. (E)

SECTION 15.1.4 - TABLE 4

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

[Ref-2] Estimating Loss-of-Coolant Accident (LOCA) Frequencies through the Elicitation Process.
NUREG-1829. NRC. April 2008. (E)

[Ref-3] Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants.
NUREG/CR-6928. NRC. February 2007. (E)

[Ref-4] V. Roux. EPR - Reliability Study of the FA3 SEMPELL Pressurizer Safety Relief Valves.
NEPS-F DC 109 Revision C. AREVA. October 2007. (E)

[Ref-5] F. Satin. EPR – Probabilistic Analysis of Accident Sequences Caused by Interfacing Loss of Coolant Accidents.
EPSE DC 833 Revision F. AREVA. March 2006. (E)

[Ref-6] Der Bundesminister für Forschung und Technologie (BMFT) (Hrsg.): Deutsche Risikostudie Kernkraftwerke, Phase B. Verlag TÜV Rheinland GmbH. Köln. 1990.
[Minister of Research and Technology: German Safety Analysis of Nuclear Power Plants, Phase B. Publisher TÜV Rheinland GmbH. Cologne. 1990.]

[Ref-7] V. Sorel. EPR PSA Assessment of initiating event frequencies.
ENFPFC0200484. Revision A. EDF. February 2003. (E)

[Ref-8] Heterogeneous Boron Dilution - PSA demonstration of dilution accident practical elimination.
NGPS4/2003/en/0120B. TR 04/138. AREVA. December 2003. (E)

[Ref-9] European Utility Requirements for LWR Nuclear Power Plants, Volume 2: Generic Nuclear Island Requirements, Chapter 17: PSA Methodology, Revision B.
EUR Document. November 1995. (E)

[Ref-10] A Reassessment of the Frequency and Duration of Loss of Off-Site Power.
SXB-IP-096233. April 1991. (E)
(This document is a National Grid Report: NGD/SD/4/89. August 1990)

[Ref-11] Re-evaluation of Station Blackout Risk at Nuclear Power Plants, Analysis of Loss of Offsite Power Events: 1986 – 2004. NUREG/CR-6890 Volume 1.
December 2005. (E)

5. ACCIDENT SEQUENCE ANALYSIS

5.2. INTERFACING SYSTEM LOCA - V-LOCA

5.2.1. Group Description

[Ref-1] EPR – Probabilistic Analysis of Accident Sequences Caused by Interfacing Loss of coolant Accidents.
EPSE DC 833 Revision F. AREVA. March 2006. (E)

5.10. ANTICIPATED TRANSIENT WITHOUT SCRAM (ATWS)

5.10.2. Functional Safety Requirement

[Ref-1] EPR – Probabilistic Analysis of Accident Sequences Caused by Anticipated Transients Without Scram.
PSSE DC 901 Revision C. AREVA. October 2004. (E)

6. CONCLUSION

[Ref-1] Probabilistic Safety Assessments of Nuclear Power Plants (Level 1).
Safety Series No. 50-P-4. IAEA. (E)

[Ref-2] European Utility Requirements for LWR Nuclear Power Plants, Volume 2: Generic Nuclear Island Requirements, Chapter 17: PSA Methodology, Revision B.
EUR Document. November 1995. (E)