UK EPR	Title: PCSR – Sub-chapter 14.0 – Assumptions and Requirements for the PCC Accident Analyses
	UKEPR-0002-140 Issue 05

Total number of pages: 27	Page No.: I / III
Chapter Pilot: F. CERRU *Name/Initials* *Date 16-11-2012*	
Approved for EDF by: A. MARECHAL *Name/Initials* A.Le.Marechal *Date 16-11-2012*	Approved for AREVA by: G. CRAIG *Name/Initials* G Craig *Date 16-11-2012*

REVISION HISTORY

Issue	Description	Date
00	First issue for INSA information.	11-12-2007
01	Integration of technical and co-applicant review comments.	27-04-2008
02	PCSR June 2009 update: - Text clarification - Inclusion of references - Technical update including addition of information given for standard reactor states and LOOP consideration.	27-06-2009
03	Consolidated Step 4 PCSR update: - Minor editorial changes - Addition of text and reference regarding consistency between PCC/RRC and PSA initiating events (§0) - Modification of RIA criteria (§2.1, g) and update of reference - Minor update to passive single failure definition (§2.7) - Update of RCCA design (new §3, Table 2 and Figure 1 added)	28-03-2011
04	Consolidated PCSR update: - References listed under each numbered section or sub-section heading numbered [Ref-1], [Ref-2], [Ref-3], etc - Minor editorial changes - Update of standard reactor states B and C (§1.2 and Table 1) to include values for monophasic operation during start-up - Improved wording in §3.1 related to previous analyses being bounding for the improved RCCA characteristics	27-09-2012
05	Consolidated PCSR update: - Minor correction to fuel clad failure decoupling criterion (§2.1)	16-11-2012

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 14.0 – ASSUMPTIONS AND REQUIREMENTS FOR THE PCC ACCIDENT ANALYSES

0. FOREWORD

Chapters 14 to 16 present the analysis of the plant response to postulated disturbances, malfunctions or failures of equipment. Their purpose is to demonstrate that the radiological consequences of abnormal events remain below the acceptance limits.

The postulated initiating events are classified into three Plant Condition Categories (PCC-2 to PCC-4) and two Risk Reduction Categories (RRC-A and RRC-B)

The PCCs contain events caused by the failure of one component, the failure of one I&C function, one operator error, or the loss of off-site power. The safety analysis of the PCC events defines the deterministic design of the safety systems. It is addressed in Chapter 14.

The RRC events are analysed in order to provide a frame for the design of additional equipment needed to meet probabilistic objectives for core melt and large radioactive releases and to limit the radiological consequences to an acceptable level in the case of a postulated low pressure core melt.

The RRC-A events are principally related to the prevention of core melt. They are event combinations including multiple failures, such as an initiating event combined with a common cause failure of a required safety system. They are dealt with in Sub-chapter 16.1.

The RRC-B events are related to the prevention of large releases in the case of a postulated low core pressure melt. They are presented in Sub-chapter 16.2.

The PCC and RRC-A events bound the PSA initiating events [Ref-1]. Therefore, the list of PSA initiating events is consistent with that analysed in the deterministic transient analyses.

The safety analysis presented in Chapter 14 and 16 is generally based on the simulation of the plant response for the different PCC and RRC initiating events. For the current stage of the PCSR, it has not been considered necessary to simulate all initiating events, given the existence of previous EPR transient analyses performed for power levels ranging from 4250 to 4900 MWth:

- For those transients that have not been re-analysed, but are considered as potentially limiting, the safety demonstration is provided by reference to transient analyses performed at 4900 MWth in the Basic Design Report 99 (BDR-99); compliance with the acceptance criteria mainly results from:

    - The beneficial effect of a lower power level.

    - The fact that the required safety systems have identical, or similar, performances.

  A comparison of the safety systems, I&C set points, and relevant design parameters of the EPR_{4900} and EPR_{4500} is presented [Ref-2].

- For those transients that have not been re-analysed, and are not expected to be limiting or whose consequences are not highly dependent on the power level, results of simulations performed at a power level different from 4500MWth are presented for information purposes in order to illustrate the qualitative behaviour of the plant; these results are referred to as "typical" in the corresponding sections of Chapter 14.

Chapter 14 is dedicated to deterministic studies of design events:

- Sub-chapter 14.0 presents the assumptions and requirements for the PCC accident analyses,
- Sub-chapter 14.1 describes the plant characteristics taken into account in the accident analysis,
- Sub-chapter 14.2 specifies analysis of the Passive Single Failure,
- Sub-chapter 14.3 contains the analysis of PCC-2 events,
- Sub-chapter 14.4 contains the analysis of PCC-3 events,
- Sub-chapter 14.5 contains the analysis of PCC-4 events,
- Sub-chapter 14.6 presents radiological consequences calculations,
- Sub-chapter 14.7 describes the fault and protection schedule including the principles used to define the protection system setpoints
- Appendix 14A describes computer codes used for accident analysis,
- Appendix 14B gives BDR-99 safety analyses used in Chapter 14.

1. COVERED RANGE

1.1. INTRODUCTION

Events are selected according to their potential risk with regard to the main safety functions:

- Reactivity and power control,
- Decay heat removal from the fuel elements,
- Confinement of radioactivity.

They are classified into four Plant Condition Categories (PCCs) and two Risk Reduction Categories (RRCs).

Chapter 14 deals only with safety analysis of PCC events. The classification into PCCs is performed in accordance with the estimated frequency of occurrence of the events:

- PCC-1: normal operating transients
- PCC-2: design basis transients (10^{-2}/y < f)
- PCC-3: design basis incidents (10^{-4}/y < f < 10^{-2}/y)
- PCC-4: design basis accidents (10^{-6}/y < f < 10^{-4}/y)

The PCCs include events caused by the failure of a component, the failure of an I&C function, operator error or loss of off-site power.

The analysis of RRC events is addressed in Chapter 16.

The safety analysis rules and the acceptance criteria to be used for the analysis of the PCC-2 to PCC-4 events are presented in section 2 of this sub-chapter.

Some events can be classified in two different plant condition categories depending on whether they are considered during power operation or during shutdown states.

In line with the break preclusion concept discussed in Sub-chapter 5.2, the double-ended guillotine break of the main coolant line (2A-LOCA) is neither a PCC nor a RRC-A event. It is addressed using the methodology for verification of the design of the containment as discussed Sub-chapter 6.2.

Although the breaks on the main steam lines are excluded in line with the break preclusion concept, the steam system piping break is considered as a PCC-4 event. This ensures that all the failures which could occur to any pipe connected to the main steam lines are covered. The exception is for breaks with a Nominal Diameter lower than 50 mm (DN 50), considered as a PCC-3 event.

Internal and external hazards are addressed in Chapter 13.

Transients relevant to the mechanical design of the reactor coolant pressure boundary and of the SG shells, e.g. for overpressure protection, are addressed in Sub-chapter 3.4.

1.2. STANDARD REACTOR STATES

Events postulated in the safety analysis are assumed to occur during normal plant operation. The initial conditions assumed in the safety analysis cover all possible standard reactor states from full power operation to cold shutdown. The following six standard reactor states are defined (see also Sub-chapter 14.0 - Table 1).

State A:

Power states and hot and intermediate shutdown (P > 130 bar). In these shutdown states, all the necessary automatic reactor protection functions are available as in the power state. In fact, some protection functions may be deactivated at low power, but there are always sufficient automatic protection functions to meet the acceptance criteria if a transient occurs.

State B:

Intermediate shutdown above 120°C (P < 130 bar). State B covers all shutdown states during normal plant operation, where primary heat is removed by the SG. It extends from 130 bar (inhibition of some F1A signals) to 25 bar/120°C (connection of RIS/RRA [SIS/RHRS]) RCP [RCS] conditions. Above 120°C, the LHSI in RHR-mode (LHSI/RHR) is not connected to the RCP [RCS] in normal operation. More details on the LHSI/RHR connection conditions are provided in Sub-chapter 6.3. Note that the LHSI/RHR can be connected to the RCP [RCS] at 180°C, if necessary, but this is not an initial state corresponding to a normal operation and therefore it does not need to be considered as an initial state in the deterministic safety analysis. In this state B, some automatic reactor protection functions available in state A may be deactivated (see Sub-chapter 14.1 and 14.7).

State C:

Intermediate and cold shutdown with LHSI/RHR. The RCP [RCS] is closed or can be rapidly reclosed, e.g. when a vent line is open, so that the SGs can be used for decay heat removal, if necessary. The RCP [RCS] is full of water or at partial loop level e.g. for SG tubes draining and for RCP [RCS] purging. Reactor state C covers the RCP [RCS] temperature range between 120°C and 15°C. Three different sub-states C1, C2 and C3 are defined depending on the different levels of RCP [RCS] water inventory, operating status of reactor coolant pumps and LHSI/RHR pumps and SG availability for heat removal:

State C1

- RCP [RCS] pressure around 30 bar (range : 24.5 – 32 bar)
- RCP [RCS] temperature between 120°C and 100°C
- RCP [RCS] water inventory corresponding to the pressuriser level at hot zero power conditions
- two SG participating in heat removal
- two reactor coolant pumps in operation

- RIS/RRA [SIS/RHRS] operating via two LHSI/RHR trains, the other two trains are on stand-by

State C2

- RCP [RCS] pressure around 30 bar (range : 24.5 – 32 bar)
- RCP [RCS] temperature between 100°C and 15°C
- RCP [RCS] water inventory corresponding to the pressuriser level at hot zero power conditions
- two SG available for heat removal
- one or two reactor coolant pumps in operation
- RIS/RRA [SIS/RHRS] operating via all 4 LHSI/RHR trains

State C3

- RCP [RCS] pressure between 32 and 1 bar
- RCP [RCS] temperature between 15°C and 55°C
- RCP [RCS] water inventory between pressuriser level at hot zero power conditions and low level operation (3/4 loop)
- two SG available for heat removal
- No reactor coolant pumps in operation
- RIS/RRA [SIS/RHRS] operating via three LHSI/RHR trains, the other train is on standby.

State D:

Cold shutdown with RCP [RCS] open so that the SGs cannot be used for decay heat removal. The RCP [RCS] level can be at partial loop level. In state D with lowered RCP [RCS] level (operation at ¾ loop level), three out of four LHSI/RHR trains are required to be in operation to maintain a RCP [RCS] temperature below 55°C. The fourth LHSI/RHR train is on stand-by.

State E:

Cold shutdown with the reactor cavity flooded for refuelling.

State F:

Cold shutdown with the core fully unloaded. During this state works are performed on RCP [RCS] components. This state does not need to be analysed for core protection.

1.3. LIST OF PCC EVENTS

1.3.1. PCC-1 events: normal operating transients

- Plant heat up and cooldown
- Step load changes
- Ramp load changes
- Load reduction up to and including the design full load rejection
- Loss of the main grid connection with the auxiliary grid connection available
- Loss of the main feedwater system with the start-up and shutdown system available
- Partial reactor trip

These operational transients are assumed to occur regularly in the course of normal operation. These events are not submitted to the safety analysis but are used to define the loading conditions for the RCP [RCS] and the Main Steam and Feed Water System.

1.3.2. PCC-2 events: design basis transients[1]

3.1 - ARE [MFWS] malfunction causing a reduction in feedwater temperature

3.2 - ARE [MFWS] malfunction causing an increase in feedwater flow

3.3 - Excessive increase in secondary steam flow

3.4 - Turbine trip

3.5 - Loss of condenser vacuum

3.6 - Short term loss of off-site power (≤ 2 hours)

3.7 - Loss of normal feedwater flow (loss of all ARE [MFWS] pumps and of the start-up and shutdown pump)

3.8 - Partial loss of core coolant flow (Loss of one reactor coolant pump)

3.9 - Uncontrolled rod cluster control assembly (RCCA) bank withdrawal at power

3.10 - Uncontrolled rod cluster control assembly (RCCA) bank withdrawal from hot zero power conditions

3.11 - RCCA misalignment up to rod drop, without limitation

3.12 - Start-up of an inactive reactor coolant loop at an incorrect temperature

[1] When the initial reactor state is not mentioned, it is assumed to be power state A.

3.13 - RCV [CVCS] malfunction that results in a decrease in boron concentration in the reactor coolant

3.14 - RCV [CVCS] malfunction causing increase or decrease in reactor coolant inventory

3.15 - Primary side pressure transients (spurious pressuriser spraying, spurious pressuriser heating)

3.16 - Uncontrolled RCP [RCS] level drop (states C, D)

3.17 - Loss of one cooling train of the RIS/RRA [SIS/RHRS] in RHR mode (states C, D)

3.18 - Loss of one train of the fuel pool cooling system (PTR [FPCS]) or of a supporting system (state A)

3.19 - Spurious reactor trip (state A)

1.3.3. PCC-3 events: design basis incidents[2]

4.1 - Small steam or feedwater system piping failure (≤ DN 50) including break of connecting lines (no greater than DN 50) to SG

4.2 - Long term loss of off-site power (> 2 hours)

4.3 - Inadvertent opening of a pressuriser safety valve

4.4 - Inadvertent opening of a SG relief train or of a safety valve (state A)

4.5 - Small break LOCA (not greater than DN 50) including a break occurring on the extra boration system injection line (states A and B)

4.6 - Steam generator tube rupture (1 tube)

4.7 - Inadvertent closure of one/all main steam isolation valves

4.8 - Inadvertent loading and operation of a fuel assembly in an improper position

4.9 - Forced decrease of reactor coolant flow (4 pumps)

4.10 - Leak in the gaseous or liquid waste processing systems

4.11 - Loss of primary coolant outside the containment

4.12 - Uncontrolled RCCA bank withdrawal (states B, C and D)

4.13 - Uncontrolled single control rod withdrawal

4.14 - Long term loss of off-site power (> 2 hours), fuel pool cooling aspect (state A)

4.15 - Loss of one train of the fuel pool cooling system (PTR [FPCS]) or of a supporting system (State F)

---

[2] When the initial reactor state is not mentioned, it is assumed to be power state A.

4.16 - Isolable piping failure on a system connected to the fuel pool (states A to F)

1.3.4. PCC-4 events: design basis accidents[3]

5.1 - Long term loss of off-site power in state C (> 2 hours)

5.2 - Steam system piping break

5.3 - Main Feedwater system (ARE [MFWS]) piping break

5.4 - Inadvertent opening of a SG relief train or safety valve (state B)

5.5 - Spectrum of RCCA ejection accidents

5.6 - Intermediate and large break LOCA (up to the surge line break, in states A and B)

5.7 - Small break LOCA (not greater than DN 50) including a break in the RBS [EBS] injection line (states C and D)

5.8 - Reactor Coolant Pump seizure (locked rotor)

5.9 - Reactor Coolant Pump shaft break

5.10 - Steam Generator tube rupture (2 tubes in 1 SG)

5.11 - Fuel handling accident

5.12 - Boron dilution due to a non-isolable rupture of a heat exchanger tube

5.13 - Rupture of systems containing radioactivity in the Nuclear Auxiliary Building

5.14 - Isolable safety injection system break (≤ DN 250), in residual heat removal mode (states C, D)

5.15 - Non-isolable small break (≤ DN 50) or isolable safety injection system break (≤ DN 250) in residual heat removal mode - fuel pool drainage aspect (State E)

1.4. PCC OPERATING CONDITIONS ANALYSED IN THE SAFETY REPORT

Some of the PCC-2, PCC-3 and PCC-4 events listed in sub-section 1.3 of this sub-chapter are covered by other events in terms of the potential effects on safety. They will not be specifically studied in Chapter 14, provided this approach can be justified.

[3] When the initial reactor state is not mentioned, it is assumed to be power state A.

2. PCC ACCIDENT ANALYSIS RULES

The safety analysis rules provide a conservative methodology to demonstrate the safety systems are designed in an appropriate manner. The level of conservatism in these rules is selected to provide appropriate design margins. The safety analyses, thermal hydraulic and neutronic transient calculations, of Chapter 14 and radiological calculations of Sub-chapter 14.6 demonstrate the suitability of the design. They refer to the deterministic safety assessment of the Nuclear Power Plant.

A global probabilistic safety assessment is also carried out, in order to demonstrate compliance with general safety objectives. This is presented in Chapter 15.

The safety analysis rules defined in this section, are named “PCC accident analysis rules”, since they are used to perform the PCC accident analyses of Chapter 14. These rules are strictly applied when calculating the thermal hydraulic and neutronic transients associated with the PCC incidents and accidents. They cover the initiating events of PCC-2, PCC-3, and PCC-4.

The “PCC accident analysis rules” are part of the conservative methodology which supports the deterministic safety assessment of the Nuclear Power Plant.

2.1. ACCEPTANCE CRITERIA

Acceptance criteria are assigned to each PCC accident or family of accidents. Compliance with these acceptance criteria ensures that the safety objectives relevant to the PCC accident are met.

The acceptance criteria are divided into safety criteria and decoupling criteria.

<u>Safety criteria</u>

Safety criteria are defined in terms of radiological limits. They must be met in the safety analysis. The most stringent criteria apply to the most probable events, i.e. those of PCC-2.

The radiological limits for PCC-2 are those of normal operation. They are defined in the section related to General Design Principles, Sub-chapter 3.1.

There is no difference between PCC-3 and PCC-4 in terms of the radiological limits as presented in Sub-chapter 3.1.

Data and assumptions used for the radiological calculations are described in the section related to Radiological Consequences, Sub-chapter 14.6.

<u>Decoupling criteria</u>

In addition to safety criteria, it is convenient for practical purposes to introduce some decoupling criteria, which may be applied to the thermal hydraulic and neutronic calculations. This allows the thermal hydraulic and neutronic calculations to be decoupled and carried out separately from the radiological calculations.

Decoupling criteria are defined such that meeting them ensures that the safety criteria, i.e. the radiological limits, will also be met.

Decoupling criteria must be met while applying all conservative “PCC accident analysis rules”.

The following decoupling criteria are used in the PCC accident analyses [Ref-1]:

a) There must be no fuel clad failure in any PCC-2 event, or in the PCC-3/PCC-4 events involving a failure of the secondary side pressure boundary at hot shutdown, e.g. main steam line break, for which there is a power increase during the transient. The decoupling criterion is “no Departure from Nucleate Boiling (DNB)”.

b) The number of fuel rods experiencing DNB for other PCC-3/PCC-4 events must remain below 10%.

c) Decoupling criteria for LOCA:

- peak clad temperature must remain below 1200°C,
- maximum clad oxidation must remain lower than 17% of the clad thickness,
- maximum hydrogen generation must remain below 1% of the amount which would be generated if all the active part of the clad had reacted,
- core geometry must remain coolable, i.e. calculated changes in core geometry must be such that the core remains capable of being cooled,
- long term core cooling must be demonstrated. The calculated core temperature must be maintained at an acceptable low value and decay heat removed.

d) Peak clad temperature must remain below 1482°C for fast transients which do not involve fuel clad oxidation.

e) Maximum linear power density must remain below 590 W/cm in PCC-2 events.

f) Fuel melting at the hot spot must not exceed 10% by volume for PCC-3/PCC-4. Less than 10% of the cross section of the hottest fuel rod at the elevation of the power peak is allowed to reach the melting temperature.

g) Decoupling criteria for Reactivity Insertion Accidents (RIA). To meet the safety requirements, two criteria are defined [Ref-2] [Ref-3] to prevent any safety concern for PCC-4 events and to maintain reactor safety during a rod ejection accident:

- The number of fuel rods over 25 GWd/te average burnup experiencing DNB must remain below 10%.
- The cladding failure limit is expressed in terms of average fuel enthalpy rise (cal/g) and depends on the initial linear power density. For every average rod burnup between 0 and 69 GWd/te, the maximum average fuel enthalpy rise (cal/g) at the peak power node is expressed with the following formulae:

$$\Delta H_{\max}(BU) = Min\left(162.26\,;141.4 - 29 \times \tanh\left(\frac{BU-49}{8.5}\right)\right) \text{ if } LPD_{init} = 0 \text{ W/cm}$$

$$\Delta H_{\max}(BU) = Min\left(151.56\,;151.56 - 48.5 \times \tanh\left(\frac{BU-45}{12}\right)\right) \text{ if } LPD_{init} < 100 \text{ W/cm}$$

$$\Delta H_{\max}(BU) = Min\left(134.49\,;149.19 - 60 \times \tanh\left(\frac{BU-44.7}{15.1}\right)\right) \text{ if } LPD_{init} < 200 \text{ W/cm}$$

$$\Delta H_{\max}(BU) = Min\left(123.68\,;108.66 - 35.6\times\tanh\left(\frac{BU-54.6}{11.1}\right)\right)$$ if $LPD_{init} < 300$ W/cm

$$\Delta H_{\max}(BU) = Min\left(108.43\,;110.75 - 51\times\tanh\left(\frac{BU-49.9}{9.9}\right)\right)$$ if $LPD_{init} < 400$ W/cm

$$\Delta H_{\max}(BU) = Min\left(102.12\,;99.15 - 49\times\tanh\left(\frac{BU-49.9}{9.9}\right)\right)$$ if $LPD_{init} < 450$ W/cm

In addition, protection against primary and secondary system overpressures must be demonstrated as discussed in section 1.5 of Sub-chapter 3.4.

For accidents occurring during cold shutdown, the initial state of various barriers may be different from that during power operation. For instance the containment or the RCP [RCS] may be open. The decoupling criteria related to barrier integrity will be adapted accordingly and is discussed in the relevant sections.

2.2. SAFE STATES

The safety analysis must be performed until a safe state is reached. Two states are defined: the controlled state and the safe shutdown state as discussed in section 1 of Sub-chapter 3.2.

For each PCC, it must be demonstrated that the controlled state can be reached. The analysis of the transition from the controlled state to the safe shutdown state may be performed once per set of similar PCCs.

2.3. METHODOLOGY

A PCC study must show that the safety criteria are met with a high confidence level. When uncertainties relating to the result are quantified, the confidence must be equal to at least 95%.

A methodology may be defined as a set of procedures, or rules, for the calculation methods to be implemented to ensure the conservative nature of the results. The methodology must use calculation codes that are authorised and appropriate for the relevant physical phenomena.

The methodology to define the accident scenario is developed in several stages:

- accident initiating event definition,
- identification of dominant physical phenomena and verification of whether the calculation codes are suitable to model these phenomena,
- identification of dominant parameters and application of uncertainties and penalties within the calculations.

Uncertainties must be considered:

- either in a deterministic manner with each dominant parameter considered at its conservative value, including uncertainty,

- or in a statistical manner with the uncertainties in several parameters statistically combined.

Once this scenario is established, the systems claimed during the transient, as identified in sub-section 2.6 of this sub-chapter, are assumed to work properly. Operator errors and systems failures are considered in the PSA presented in Chapter 15.

2.4. INITIAL CONDITIONS

The initial conditions for PCC accident analysis correspond to steady state operation.

The definition of the PCC involves the definition of the standard reactor state to be considered. The standard reactor states are described in sub-section 1.2 of this sub-chapter.

Within the given standard reactor state, the most conservative operating condition is considered for assessing the PCC acceptance criteria. For example, full power operation is assumed for LOCA in state A (power operation), or the maximum RCP [RCS] pressure around 30 bar for LOCA in state C (LHSI/RHR operation).

The physical parameters are set within the limits provided by the plant controls or by the limiting conditions of operation (LCO) functions. A conservative combination of parameters is considered including uncertainties, dead-bands and response times. For each PCC event the most conservative case is analysed.

The list of PCC events covers all plant operating conditions, including shutdown states, as potential initial conditions before accidents.

2.5. RULES FOR OPERATOR ACTIONS

A distinction is made between two phases of a transient, the automatic phase and the manual phase:

- the automatic phase lasts from the event occurrence up to the first manual action,

- the manual phase lasts from the first manual action, up to the safe shutdown state.

During the manual phase, as described in Sub-chapter 3.1, manual actions are taken into account in the accident analysis, in addition to automatic actions. Operator “grace periods” are defined:

- a manual action from the Main Control Room (MCR) is assumed to take place, at the earliest, 30 minutes after the first significant information is transmitted to the operator,

- a local manual action, i.e. a manual action that must be performed outside the MCR, is assumed to take place, at the earliest, 1 hour after the first significant information is transmitted to the operator.

In the large majority of cases the controlled state will be reached using only automatic actions. However this is not mandatory. Reliance on manual actions to reach the controlled state is allowed, provided that the operator “grace periods” are met.

Operators are assumed to act according to the Emergency Operating Procedures (EOP). No operator errors are considered in the PCC accident analyses. Such errors are covered by the PSA in Chapter 15, based on human reliability models.

2.6. MECHANICAL, ELECTRICAL AND I&C SYSTEMS ADDRESSED IN THE SAFETY ANALYSIS

The safety classification concept and the related wording are defined in Sub-chapter 3.2. In the PCC accident analyses, a distinction is made between 2 types of functions:

- F1 functions, including F1A and F1B functions,
- Non-F1 functions, including F2 and NC functions.

For the PCC/RRC analyses, the functional safety classification is applied to the systems and refers to the safety function performed by the system

For example:

In section 3.5.3.3 of Sub-chapter 14.3, it is stated:

"**VIV [MSIV] (F1A):** All VIV [MSIV] are closed on « SG pressure drop > MAX1 ». The setpoint of this signal is adjusted […]. The delay for steam lines isolation consists of 0.9s channel delay plus 5s of valve closing time"

The F1A refers to the F1A safety classified function "VIV [MSIV] closure on SG pressure drop > MAX1" which is related to the VIV [MSIV].

<u>F1 functions</u>

The functions that are F1 safety classified may be used in the PCC accident analyses.

The performance of the F1 functions and related systems that are considered in the PCC studies is conservatively modelled. The effectiveness of the functions / systems is affected by consideration of:

- uncertainties on equipment characteristics,
- uncertainties on actuation setpoints,
- the worst environmental conditions, etc…

It must be shown in the PCC accident analyses that:

- the controlled state can be reached using only F1A functions, with the exception of the F1B support functions / systems listed in Sub-chapter 3.2, and
- the transfer from the controlled state to the safe shutdown state can be done using only F1A and/or F1B functions.

F2 and non-safety-classified (NC) functions

The following principles apply to F2 and NC functions used in the PCC accident analyses:

a) If the transient leads to an actuation of a F2 or NC system, and if this system would have a beneficial effect when assessing a safety criterion, the PCC accident analysis must be performed without considering this system.

b) If the transient leads to an actuation of a F2 or NC function, and if this function worsens the consequences of the accident when assessing a safety criterion, the PCC accident analysis must be performed assuming that the system operates normally.

c) If the transient has no impact on a F2 or NC functions performance, there is no change of status and no change of operating and environmental conditions, and if the function was operating prior to the accident, the system is assumed to continue normal operation. No spurious commands from the I&C need to be assumed in these conditions.

   Example: this applies to reactor coolant pumps (including their seal injection system) in the event of no loss of grid and to the I&C closed loop controls. No spurious commands from the I&C are considered in these conditions.

   Example: the SG level control by the main feedwater valves is not F1 safety classified. However, in the case of SGTR, the I&C closed loop control is not affected by the event. Therefore, this I&C function is assumed to continue working properly until the ARE [MFWS] isolation which is F1 safety classified. In particular it does not generate spurious commands leading to a full opening or closing of the ARE [MFWS] valves.

d) More generally, a F2 or NC function is assumed either to work properly or not to work at all. Incorrect operation is not considered in the PCC accident analyses.

   Example: When the main steam bypass (GCT [MSB]) is actuated and credited in the course of a transient, the valves are assumed to reclose normally and not to get stuck open.

e) The turbine isolation valves closure is not F1 safety classified but these valves are assumed to close normally after a reactor trip. This is justified because they are redundant and in series, they are operating under design conditions, and they are designed to be "fail safe". The disconnection of the main power generator after turbine trip is also assumed to occur correctly.

2.7. APPLICATION OF THE SINGLE FAILURE CRITERION (SFC) IN THE SAFETY ANALYSIS

The single failure concept is addressed in the section related to General Design Principles in Sub-chapter 3.1.

For the PCC accident analyses, the term of single failure will be understood as any active or passive failure, independent of the postulated initiating event, which affects all or part of an item of equipment used in the analysed transient. It applies to any equipment that needs a change of state to fulfil its function and that has beneficial effects on the transient.

The concept is applied on the same basis as that defined in the section dedicated to General Design Principles, Sub-chapter 3.1, for the system design, while taking into account the following:

- if a F1 function can be fulfilled by more than one safety system, including diverse or supporting systems, the single failure is applied to these systems only once.

- it must be verified in the PCC accident analysis that a single failure in the form of a leak at any location in the pressure boundary and its consequential failure does not prevent performance of the required safety function.

- If the leak cannot be detected or isolated, it must be considered as likely to develop up to the flow rate corresponding to a complete pipe break; the initial leak rate is conventionally assumed to be 200 l/min; also it must be shown that the ability to perform the safety function is not impaired.

In the PCC accident analysis, the following additional rules must be applied:

a) The most conservative single failure anywhere in the systems needed to perform the safety function must be assumed to occur.

b) Consequential failures resulting from the assumed failure must be considered as part of the single failure criterion.

⇒ If necessary, sensitivity studies must be performed for a given event with the application of the SFC to different components, to determine the most conservative single failure for assessing the safety criteria.

c) An active single failure must be considered from the beginning of the analysis. Sub chapter 14.2 also shows that the UK EPR design is robust to passive single failures considered from the start of the analysis.

d) Any exception with respect to the single failure must be stated and justified.

e) A stuck rod is considered to be an application of the SFC.

f) A spurious opening of a safety valve is considered as an initiating event.

g) The non-closure of a safety valve after actuation is considered as an application of the SFC.

2.8. PREVENTIVE MAINTENANCE

Preventive maintenance during power operation

During preventive maintenance, equipment is considered to be unavailable.

If the nature of preventive maintenance is such that the system can be restored to an operational state in due time (such that the necessary safety function can be fulfilled on demand), the system is considered to be available. Examples are short maintenance activities such as an oil change or filter replacement for some supporting systems.

If preventive maintenance of an F1 safety system is scheduled during power operation, then, in the safety analysis studies, one train must be assumed to be out of service for preventive maintenance.

Preventive maintenance during shutdown

If preventive maintenance of an F1 safety system is scheduled during shutdown, then, in the safety analysis studies, one or more trains must be assumed to be out of service for preventive maintenance, in accordance with the schedule for preventive maintenance during shutdown.

2.9. LOSS OF OFF-SITE POWER (LOOP)

2.9.1. Pre-Construction Safety Report

For the PCC studies described in the PCSR, LOOP is considered in accordance with the following specific rules:

- LOOP is combined with the PCC-3 and PCC-4 power operation events, if it is conservative. It is assumed to occur at the time of turbine trip.
- LOOP is not combined with PCC-2 power operation events or with PCC-2 to PCC-4 events during shutdown states.

2.9.2. Pre-Commissioning Safety Report

For the detailed design studies described in the Pre-Commissioning Safety Report, two cases will be distinguished for each PCC.

PCC-2 events will be studied without consideration of LOOP. PCC-3 and PCC-4 will be studied without consideration of LOOP if this assumption is penalising.

The case with consideration of LOOP will be studied in PCC-2 to PCC-4 categories with specific rules that will be detailed in the Pre-Commissioning Safety Report.

2.10. ANALYSIS RULES SPECIFIC TO PCC EVENTS ASSOCIATED WITH THE FUEL STORAGE POOL

Due to the specific nature of the fuel storage pool, it is un-pressurised and changes to physical parameters are very slow in comparison with the transients in the primary system, etc., the analysis rules for events concerning the fuel storage pool are slightly different from the analysis rules specified for the other PCC events.

2.10.1. Acceptance criteria

The safety criteria for PCC-2 to PCC-4 related to the fuel pool are as follows:

- permanent maintenance of sub-criticality,
- avoidance of exposure of fuel assemblies i.e. fuel uncovery does not occur.

For PCC-2 events, an additional criterion is to maintain a significant margin to pool water boiling. The criterion of maintaining the pool water temperature below 80°C is used to decouple this analysis.

2.10.2. Controlled state and safe state

The controlled state is characterised by the short term removal of decay heat. For faults involving a loss of a PTR [FPCS] cooling train, given the long time before possible fuel exposure, it is assumed that the controlled state is reached at the start of the transient. For fuel pool draining faults, the controlled state corresponds to a water inventory that is stabilised by stopping the draining, without any fuel being uncovered.

The safe state is characterised by the permanent removal of decay heat from the fuel stored in the pool by at least one PTR [FPCS] cooling train, with a significant margin to boiling, i.e. water temperature below 80°C.

Note: For PCC-3 and PCC-4 events, the decay heat may be transiently removed by boiling the pool water.

The safety analysis must be performed for each PCC up to the time when it can be demonstrated that the safe state has been reached.

2.10.3. Initial conditions

The initial conditions for the transient analysis correspond to an established state.

Three initial plant operating conditions are considered in the PCC event studies for the spent fuel pool: “Beginning of Cycle (BOC)”, “End of Cycle (EOC)” and “Refuelling”.

They are characterised as follows:

- “Refuelling”: once the core has been fully unloaded, the pool should be filled with fuel elements. It will contain spent fuel assemblies which have just been unloaded, new fuel assemblies for the next cycle and fuel assemblies which were unloaded on completion of previous cycles.

- “BOC” (Beginning of Cycle): the content of the fuel storage pool equals the difference between the content in the “refuelling” state and the content of the core that has just been reloaded in the reactor for the following cycle.

- “EOC” (End of Cycle): the content of the fuel storage pool is identical to that of the “BOC” condition, apart from the fact that the decay heat to be considered is calculated when the preventive maintenance starts to be implemented as discussed in sub-section 2.10.7 of this sub-chapter.

To remain conservative, the transient pool temperature calculations make a suitable allowance for uncertainties in the decay heat.

2.10.4. Rules for operator actions

The PCC analysis can claim a manual action from the Main Control Room no earlier than 30 minutes after the first item of significant information has been received by the operator. A local manual action, i.e. a manual action that must be performed outside the main control room, may be assumed no sooner than 1 hour after receipt of the first item of significant information.

An exception to this general rule deals with the safe positioning of a fuel assembly whilst being handled: this action, which is performed by personnel already on site at the time of transient initiation, may be considered 15 minutes after the relevant personnel have received the first item of significant information.

In addition, repair times for failed items of equipment may be introduced to the safety analysis.

2.10.5. Systems to be used during the safety analysis

The two principal PTR [FPCS] trains are F1B classified. The general rules for PCC studies specify that the safety analysis for PCC events must only be based on the use of F1 systems.

However, due to the specific nature of the spent fuel pool, high thermal inertia and low pressure, some exceptions may be introduced to this rule in order to mitigate a limited number of specific PCC events. For these events, F2 systems that have beneficial effects may be claimed in the safety analysis. The use of these F2 systems must be appropriately justified and adequate performance requirements must be defined for the relevant equipment.

2.10.6. Application of the single failure criterion

For analysis of PCC events in the fuel storage pool, the single failure to be considered is assumed to be any <u>active</u> single failure, as defined in sub-section 2.7 of this sub-chapter, independent of the assumed initiating event, affecting all or part of an item of equipment used in the transient in question.

Due to the specific nature of the pool water cooling system, operating at low pressure, its in-service inspection programme etc, no passive failures are assumed for the PTR [FPCS] itself in the safety analysis for spent fuel pool PCC events.

2.10.7. Consideration of preventive maintenance

PTR [FPCS] preventive maintenance is programmed when the grace period before boiling in the spent fuel pool is long enough. The time taken for boiling to start depends both on the decay heat and the cooling water temperature.

In the PCC studies, preventive maintenance is assumed to be performed at end of cycle (EOC) conditions, when the decay heat in the spent fuel pool is at its lowest, but whilst assuming a conservatively high cooling water temperature.

In practice, higher decay heat may be fully compensated by a lower cooling water temperature, so that PTR [FPCS] preventive maintenance can be programmed earlier in the cycle.

PTR [FPCS] preventive maintenance is not performed during refuelling shutdowns, but maintenance of the supporting systems may be carried out during these periods. Suitable measures must be implemented on the support systems in order to keep the trains separate and independent.

Periodic tests are assumed to be performed during power operation, by switching from one PTR [FPCS] train to another. As a result, the periodic tests have no impact on the accident studies.

2.10.8. Loss of off-site power (LOOP)

In the specific case of spent fuel pool water cooling, the LOOP is taken to occur at the same time as the initiating event.

Certain specific rules are applied to these studies:

- F1 and F2 equipment may be used for the safety analysis, provided they are seismic classified,
- The safety criteria to be followed are those of the PCC-4 category,
- A single failure is not applied, unless the initiator can result from the failure of a non-seismic classified component. (Otherwise, the LOOP itself is considered to be a single failure which is independent of the initiating event).

3. ROD CLUSTER CONTROL ASSEMBLY (RCCA) DESIGN

Following layout considerations, there is a need to reduce the length of the RCCA drive rods. In response to this requirement, a new design of the rods has been proposed, which meets the following objectives:

- to increase the rod weight to, at the minimum, maintain global mobile mass,
- to maintain or increase the RCCA neutronic efficiency,
- to maintain the applicability of experience feedback from the Harmoni™ RCCA.

The modification consists of increasing the RCCA cladding inner diameter as well as the absorber rod diameter, with the RCCA outer diameter remaining unchanged. The AIC rod length is also increased and the B4C rod length shortened. The developments are summarised in Sub-chapter 14.0 - Table 2. The RCCA pattern has also been modified as indicated in Sub-chapter 14.0 – Figure 1; the central RCCA is now a shutdown rod rather than a control rod.

The impact on the overall RCCA efficiency is estimated to be an increase of about 5% in the RCCA worth used to evaluate the shutdown margin.

3.1. IMPACT ON NON REACTIVITY INSERTION ACCIDENTS

For all non reactivity insertion transients, this modification leads to an increased shutdown margin and thus enhances the mitigation against the fault. There are no negative effects resulting from this modification.

The former RCCA characteristics are used in the transient analyses presented in Chapters 14 and 16. Due to the improved RCCA characteristics (integral reactivity worth improved from 4000 pcm to 5100 pcm with one rod stuck), results based on the former characteristics are conservative. The following two fault studies are an exception as they are based on the new RCCA design:

- Steam Line Break (Sub-chapter 14.5, section 2)

- Transients regarding diversity (Sub-chapter 16.5)

3.2. IMPACT ON REACTIVITY INSERTION ACCIDENTS

For reactivity insertion due to RCCA ejection or withdrawal, the new configuration is more onerous than the former one. Impacted accidents are the following:

- **Spectrum of RCCA ejection accidents** (Sub-chapter 14.5 section 5):
  This transient takes into account the new design of the RCCAs and the new RCCA pattern.

Note: Transients regarding diversity (Sub-chapter 16.5) are performed with the new design and pattern. Other reactivity insertion accidents are not impacted by the RCCA modifications:

- **Uncontrolled RCCA bank withdrawal at power** (Sub-chapter 14.3 section 9):
  This study is performed with a parametric methodology independent of the RCCA characteristics.

- **Uncontrolled RCCA bank withdrawal from hot zero power conditions** (Sub-chapter 14.3 section 10):
  The modification of the RCCA design and pattern do not have a significant impact on the large safety margin for this fault, presented in the PCSR.

- **Uncontrolled single control rod withdrawal** (Sub-chapter 14.4 section 13):
  This fault is used to assess the uncertainties associated with the use of SPNDs: the potential need for modification of the SPND uncertainties will be accommodated by site-specific setpoint re-evaluation with no consequences on the safety analyses. The new design and pattern have no impact on PCSR results.

SUB-CHAPTER 14.0 – TABLE 1

Standard reactor states

Reactor state	RIS/RRA [LHSI/RHRS]connected to CPP [RCPB]	CPP [RCPB] condition	Level of RCP [RCS] coolant	Average CPP [RCPB] temperature	CPP [RCPB] pressure	Condition of containment air lock	Comments
A	no	Closed (1)	Full	311 °C to 120 °C	155 bar abs to 130 bar abs	Closed (above ≈ 90°C in the RCP [RCS])	All of the automatic protection functions are available, as during power operation.
B					130 bar abs to 25 bar abs		Some automatic protection functions concerning the LOCA or the over-cooling transients may be deactivated below 130 bars
C	yes			120°C to 15 °C	32 bar abs to 0.2 bar abs		RIS/RRA [SIS/RHRS] connected to CPP [RCPB] at 120^{0}C during normal operation but may be connected up to 180^{0}C if necessary. At least 2 SG available for residual heat removal. 3/4 loop operation for SG tube drainage and CPP [RCPB] purging.
			3/4 loop	15 to 55 °C	atmospheric	Open (below ≈ 90°C in the RCP [RCS])	
D		Open		15 to 50 °C		Closed (2)	Handling of vessel cover: level near top of loops. Work on primary pump seals. level at ¾ loop operation.
E (3)			Full pool			Open	Core reloading.

(1) In state C, the CPP (RCPB) may be partially open (for example, vent line) but must be able to be re-closed quickly.
(2) During 3/4 loop operation after core reloading, the containment may be opened.
(3) State F is similar to State E; the only difference is that the core is fully unloaded.

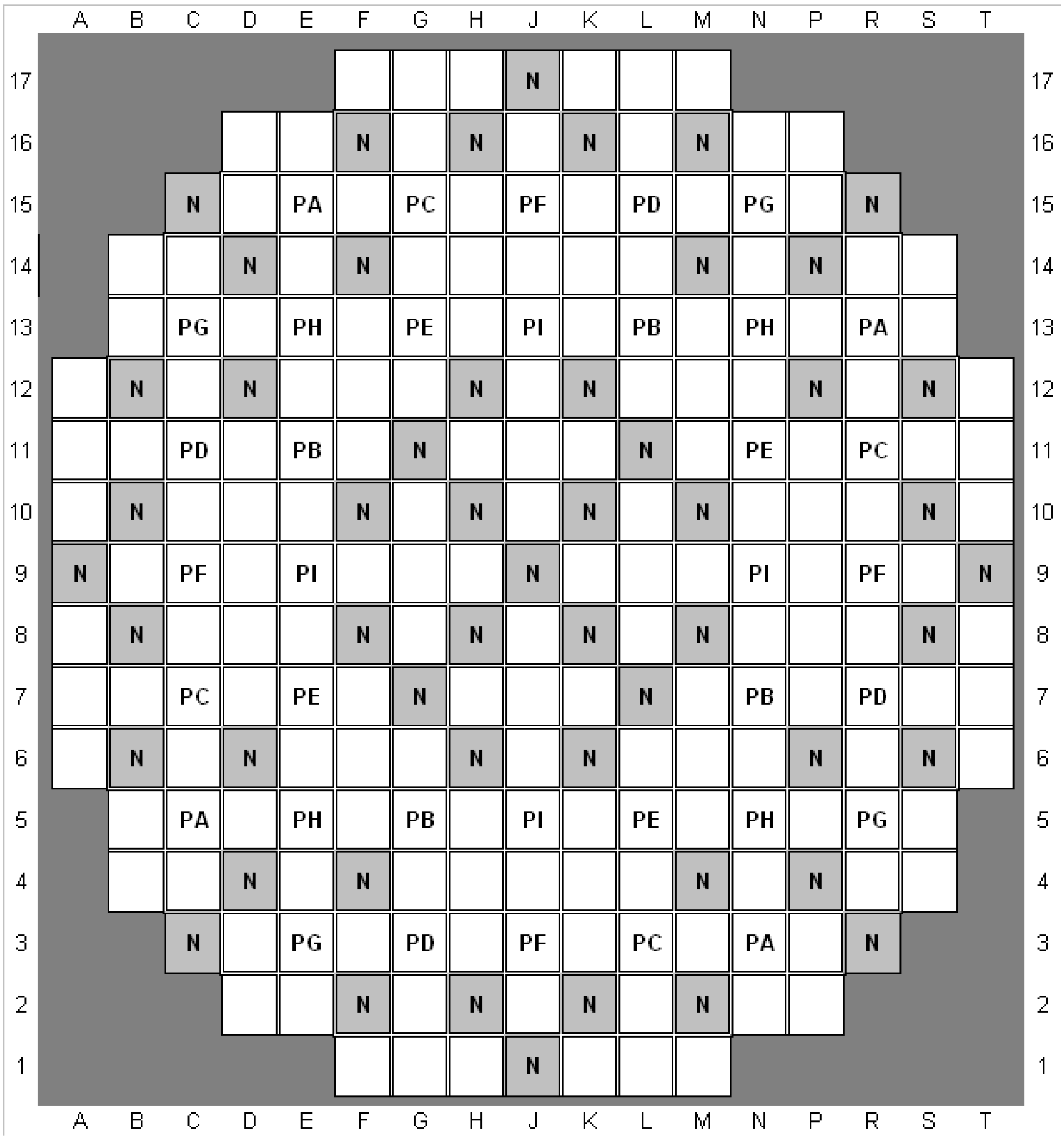
SUB-CHAPTER 14.0 – TABLE 2

RCCA characteristics [Ref-1]

Nominal dimensions	FA3 PSAR / UK 2008 DF configuration	Revised configuration
AIC length	1500 mm	2900 mm
Absorber material length	4110 mm	4240 mm
AIC length with reduced diameter	0 mm	500 mm
Cladding, outer diameter	9.68 mm	Unchanged (9.68 mm)
Cladding, inner diameter	7.72 mm	8.74 mm
Cladding thickness	0.97 mm	0.47 mm
AIC diameter (upper part)	7.64 mm	8.66 mm
AIC diameter (lower part)	7.64 mm	8.53 mm
B4C diameter	7.47 mm	8.47 mm

SUB-CHAPTER 14.0 - FIGURE 1

Rod Cluster Control Assembly pattern following RCCA design modification



	P1	P2	P3	P4	P5
S1	PA	PB	PC PD	PF PE	PG PH PI
S2	PD	PH	PC PB	PA PF	PE PG PI
S3	PF	PB	PA PE	PC PD	PG PH PI
S4	PC	PH	PD PB	PA PE	PF PG PI

SUB-CHAPTER 14.0 – 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.

0. FOREWORD

[Ref-1] V. Verreman. Consistency between PSA list and PCC list. NEPR-F DC 584 Revision A. AREVA. July 2010. (E).

[Ref-2] R Gagner. EPR sizing at 4500MWth. EPRR DC 1685 Revision C. AREVA. February 2004. (E).

2. PCC ACCIDENT ANALYSIS RULES

2.1. ACCEPTANCE CRITERIA

<u>Decoupling criteria</u>

[Ref-1] Nuclear Fuel - Specification and Justification of Design and Safety Criteria. FS1-0000607 Revision 3.0. AREVA. October 2010. (E)

[Ref-2] EPR-UK : Fuel rod PCMI failure criterion for RCCA ejection fault studies. ENCNTC100060 Revision B. EDF. September 2010. (E)

[Ref-3] M Ishikawa, S Shiozawa. A study of fuel behaviour under reactivity initiated accident conditions – review. Journal of Nuclear Materials, Volume 95. November 1980. (E)

SUB-CHAPTER 14.0 – TABLE 2

[Ref-1] EPR HARMONI® RCCA - Description, Functional Requirements and Materials Properties. FF DC 05182 Revision B. AREVA. July 2009. (E)