UK EPR	Schedule	pter 14.7 – Fault and Protection PR-0002-149 Issue 03
Total number of pages	s: 61	Page No.: I / III
Chapter Pilot: F. CER	RU	
Name/Initials	Date 26-11-2012	
Approved for EDF by:	A. MARECHAL	Approved for AREVA by: G. CRAIG
Name/Initials A.Je.N	Maeld Date 26-11-2012	Name/Initials Glowing Date 26-11-2012

REVISION HISTORY

Issue	Description	Date
00	First issue.	27-06-2009
01	Removal of RESTRICTED classification	11-06-2010
02	 Consolidated Step 4 PCSR update: Minor editorial changes Update and addition of references Consistency with UK classification approach New section 4 added, "Adequacy of design to protect the plant against faults – ALARP discussion" added 	29-03-2011
03	 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 Fault Schedule (Table 1) to reflect changes in classification, new PCC events, diversity analyses Update of Appendix 1 to cover diverse means available to reach a long-term safe shutdown state 	26-11-2012

UK EPR

Title: PCSR – Sub-chapter 14.7 – Fault and Protection Schedule

UKEPR-0002-149 Issue 03

Page No.: II / III

Copyright © 2012

AREVA NP & EDF All Rights Reserved

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 EPRTM 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.

All intellectual property rights in the content of this document are owned by AREVA NP, EDF SA, their respective affiliates and their respective licensors. You are permitted to download and print content from this document solely for your own internal purposes and/or personal use. The document content must not be copied or reproduced, used or otherwise dealt with for any other reason. You are not entitled to modify or redistribute the content of this document without the express written permission of AREVA NP and EDF SA. This document and any copies that have been made of it must be returned to AREVA NP or EDF SA on their request.

Trade marks, logos and brand names used in this document are owned by AREVA NP, EDF SA, their respective affiliates or other licensors. No rights are granted to use any of them without the prior written permission of the owner.

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 **UK EPR**

Title: PCSR – Sub-chapter 14.7 – Fault and Protection Schedule

Page No.: III / III

TABLE OF CONTENTS

- 1. LIST OF INITIATING EVENTS
 - 1.1. INTRODUCTION
 - 1.2. NSSS DESIGN CONDITIONS (PCC EVENTS)
 - 1.3. CORE MELT RISK REDUCTION CATEGORY (RRC-A EVENTS)
 - 1.4. SEVERE ACCIDENTS (RRC-B EVENTS)
 - 1.5. CONCLUSIONS
- 2. JUSTIFICATION OF THE COMPREHENSIVENESS OF FAULT PROTECTION
 - 2.1. INTRODUCTION
 - 2.2. DEFENCE IN DEPTH
 - 2.3. DEFENCE LINES
- 3. PROTECTION SYSTEM I&C ARCHITECTURE
 - 3.1. SAFETY FUNCTIONS
 - 3.2. TYPES OF I&C FUNCTIONS
 - 3.3. BASIS FOR THE DEFINITION OF AN I&C FUNCTION
 - 3.4. SET OF I&C FUNCTIONS
 - 3.5. RESET OF AUTOMATIC PROTECTION FUNCTIONS
 - 3.6. PERMISSIVE SIGNALS
- 4. ADEQUACY OF DESIGN TO PROTECT THE PLANT AGAINST FAULTS ALARP DISCUSSION
 - 4.1. OVERVIEW OF PLANT PROTECTION
 - 4.2. ANALYSIS OF FUNCTIONAL DIVERSITY
 - 4.3. RADIOLOGICAL CONSEQUENCES
- 5. CONCLUSION

APPENDIX 1: DIVERSITY IN EMERGENCY OPERATING PROCEDURE

UK EPR

SUB-CHAPTER : 14.7

PAGE : 1 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 – FAULT AND PROTECTION SCHEDULE

This sub-chapter provides a summary of the fault and protection schedule for the UK EPR. It also gives an insight into the principles used to define the protection system set-points and those applied to modify or deactivate settings during changes in the reactor state. Sections 1 and 2 of this sub-chapter describe the fault and protection schedule, which illustrates two main features of the EPR design:

- the rationale and justification for the initiating events considered within the EPR design of protection and mitigation provisions due to their potentially unacceptable consequences (section 1);
- the different defence lines provided by the EPR design. Section 2 provides a justification of the comprehensiveness of the fault protection. The fault and protection schedule is given in Sub-chapter 14.7 Table 1, which includes the initiating events and sequences, their frequencies, the classified safety systems that protect against them and the overall protection claims.

The fault schedule focuses on risks to the public; therefore, the fault schedule is based on the accidents described in Chapters 14 and 16. It also includes the analysis of the functional diversity of Sub-chapter 16.5.

Section 3 of the present sub-chapter provides information on the protection system settings and the principles applied to the deactivation or resetting of protection settings at low power states.

Section 4 of this sub-chapter provides information on the ALARP discussion regarding the adequacy of the UK EPR design to protect the plant against faults.

Section 5 of this sub-chapter provides an overall conclusion.

PAGE : 2 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

1. LIST OF INITIATING EVENTS

1.1. INTRODUCTION

UK EPR

As an evolutionary reactor, the list of design basis faults considered within the EPR design basis is based on an initial list of design basis faults considered in early PWRs and additions arising from 30 years of operational feedback from international PWR fleet (studies, operations and interaction with safety authorities). Incorporation of experience feedback has provided the list of design basis faults considered with some additional robustness.

With regard to NSSS internal events (fault studies) a review of the initial basis for the fault schedule, and the main subsequent additions, are provided below.

1.2. NSSS DESIGN CONDITIONS (PCC EVENTS)

The initial approach to the PCC event list was an implementation of the principles set out by the committee N-18 of the American Standards Institute (ANSI N-18, 1973). Based on the defence in depth concept (three levels at that time), it introduced a categorisation of internal events based on a rough concept of "anticipated frequency" (based on the frequency expected in operation during plant life and from consideration of bounding hypothetical events).

FRATEC 01 (1979) [Ref-1] presents the FRAMATOME methodology for the definition of the initiating events list and the basis for its claim to provide an exhaustive list of faults. A comparison is also made to the application of the ANSI N-18 for US PWRs. After defining normal operating parameters, events which could cause them to vary outside of normal bounding values are identified, without trying to enumerate all the failures liable to adversely affect the nuclear steam supply system. These events are arranged into several families regarding the operating parameter they first affect. The more significant transient of each family with respect to challenges to the protection system and engineered safety feature is finally considered as a design basis event or accident.

It should be noted that the aim of PCC analysis is to define the design requirements for safety systems (protection systems for category 2 events and main safeguard systems for category 3 and 4 events), which are designed subject to specific stringent rules such as the Single Failure Criterion (SFC), and the assumption of bounding consequences. This is why the consideration of additional scenarios, that were not included in the initial list, has not led systematically to a change in the list, since the additional design provisions required to reach an acceptable level of consequences may not impact on the performance of main systems or the bounding consequences of the event.

For example, the interface Loss Of Coolant Accident (LOCA) did not challenge the initial design of the Safety Injection System (RIS [SIS]) based on "normal" LOCA, or the definition of bounding bypass consequences via Steam Generator Tube Rupture (SGTR), and consequently it was not added to the PCC list. Similarly when, with the introduction of the EPR, the definition of PCCs was extended to introduce the concept of a frequency range, no significant update of the list of PCC events analysis was required.

SUB-CHAPTER : 14.7

PAGE : 3 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

The main subsequent additions to the FRATEC 01 approach were linked to changes in "design rules" (e.g. SFC, i.e. redundancy requirement at the component level) shifting to "safety analysis rules" (e.g. the requirement to assume an "aggravating failure" i.e. a redundancy requirement at the function level). Other examples were extension of the scenario duration through the operator action phase, and the introduction of additional event combinations involving Loss Of Offsite Power (LOOP).

Changes to the list of events were made related to the experience feedback and changes in system design options.

EPR specific options led to transients being added or excluded from the Design Basis Assessment (DBA) list that was used for in service French Nuclear Power Plants (NPP). The changes were in three main categories as follows:

1) Changes resulting from EPR constitutive options, such as:

UK EPR

- consideration of transients occurring in the different plant states led to PCC events for outages being introduced as design basis accidents (these were considered as beyond design basis accidents in previous French NPPs, and consequently analysed using less stringent rules);
- consideration of transients in auxiliary buildings, which led to the introduction of fuel pool transients, and transients in the effluent treatment building and the nuclear auxiliary building.

2) Changes due to design improvements in the EPR that had a direct impact on the list of design basis faults. An example was application of the break preclusion principle that led to the exclusion of 2-A LOCA from the PCC list. LOCA outside the containment was added to the DBA list to address the specific EPR design of the residual heat removal system function, which is provided by the safety injection system.

3) Changes due to the application of PSA early in the design process, which impacted on the justification of the list itself and on the way transients were arranged into the different PCC categories.

The use of PSA also impacted the list of RRC-A events considered, as mentioned below.

1.3. CORE-MELT RISK REDUCTION CATEGORY (RRC-A EVENTS)

The origin of the list of scenarios involving multiple failures (called RRC-A sequences in the EPR approach) was a French Safety Authority (ASN) request for consideration of design extension conditions representative of the total loss of main redundant systems (power supply, heat sink, SG feedwater, long term RIS [SIS] and reactor trip through Anticipated Transients Without Scram). PCC-4 criteria were imposed, but less stringent rules were accepted.

Later on, other scenarios were added at the request of the ASN, generally to illustrate the robustness of the defence in the EPR design (drainage of two SGs, initially corresponding to the SFC exception on main steam isolation valves; multiple SGTRs combined with Main Steam Line Break).

SUB-CHAPTER : 14.7

PAGE : 4 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

Eventually, a connection was made with the probabilistic analysis, and with the periodic safety review process, by considering the main PSA level 1 sequences (see PCSR Sub-chapter 15.1). The concept of an RRC-A feature was introduced to give assurance that any system making a significant contribution to reduction in the core melt risk would be safety classified. The corresponding RRC-A list has thus become a self-evolving list, on the basis of the PSA revisions issued for the purpose of periodic safety reviews. The current status of this EPR list is a combination of the initial deterministic approach and of an early implementation of the probabilistic definition. The justification for the claim that the initiating event list used in the Level 1 PSA is comprehensive is presented in section 4 of Sub-chapter 15.1 (NSSS internal events).

1.4. SEVERE ACCIDENTS (RRC-B EVENTS)

The main characteristics of the EPR design approach to severe accidents are:

- postulated low-pressure core melt scenarios are defined to support the design of dedicated mitigation systems (RRC-B features list);
- "Practical elimination" (IAEA terminology) of large early releases is sought via design measures introduced to prevent direct containment heating, prompt criticality, steam and hydrogen explosions, containment bypass, fuel melting in the fuel building. Probabilistic calculations are may be used to justify design measures, but cannot be used in isolation, without corresponding design measure being introduced;
- specific stringent radiological criteria are associated with severe accidents consequences (limited need for sheltering or food restrictions, no need for emergency evacuation or permanent relocation in the vicinity of the site);
- global design effectiveness is confirmed via a level 2 PSA.

1.5. CONCLUSIONS

UK EPR

The list of PCC and RRC events considered in the EPR safety approach arises from two objectives: compliance with design rules (main protection and safeguard systems) and demonstration by safety analyses. An absolute claim on the exhaustiveness of the event lists considered is not possible. However the extensive review and development of the event lists over many years, and the recent use of PSA analyses, give confidence that this mainly deterministic design approach has captured the potential consequences of all significant initiating events that could occur.

PAGE : 5 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

2. JUSTIFICATION OF THE COMPREHENSIVENESS OF FAULT PROTECTION

2.1. INTRODUCTION

UK EPR

In this section, the safety measures are identified and justified and their consistency with defence in depth concept is explained.

This chapter identifies the safety functional requirements applicable to the safety measures, the categorisation of the functions, and the classification of the systems, structures or components that contribute to the safety measure. A distinction is made between the lines of defence (first line consisting of preventive measures, main line consisting of protective measures and back up line consisting of back-up safety measures).

The safety measures described in this chapter are illustrated and detailed for each transient considered, in Sub-chapter 14.7 – Tables 1 and 2. For each initiating event, the fault schedule table gives the associated Plant Condition Category (PCC) or Risk Reduction Category (RRC) which bounds the resulting fault transient. It also identifies the PCSR section where the fault transient is considered, and, for each phase of the transient, the protection systems which perform the different required safety functions in the different defence lines.

2.2. DEFENCE IN DEPTH

A defence in depth concept, described in Sub-chapter 3.1, is applied at the design stage of the EPR. It leads to the implementation of five levels of defence in the engineered safety systems and components, as follows:

- level 1 is a combination of conservative design, quality assurance, high quality of fabrication and high level of surveillance activities (controls, monitoring) to prevent departures from normal plant operation;
- level 2 consists of the implementation of protection devices which make it possible to detect and correct the effects of deviations from normal operation or the effects of system failures. This defence level is aimed at ensuring the integrity of the fuel cladding and that of the primary cooling system so as to prevent anticipated operational occurrences from escalating to accident conditions;
- level 3 consist of safeguard systems, protection devices and operating procedures which make it possible to control the consequences of accidents that may occur so as to contain radioactive material and prevent occurrence of severe accidents;
- level 4 comprises measures aimed at preserving containment integrity and controlling severe accidents;
- level 5 includes, in the event of the failure of previous levels of defence, all measures for protecting the public against the effects of significant radiological discharges.

SUB-CHAPTER : 14.7

PAGE : 6 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

Defence levels 2 and 3 are the only ones relevant to the lines of defence considered in the fault analysis. The preventive line of defence, as described below, is associated with level 2, while both the main and back-up lines of defence are associated with level 3. Note that it is not the purpose of the present sub-chapter to consider mitigation of severe accidents, radiological consequences or containment integrity (third barrier) issues.

2.3. DEFENCE LINES

UK EPR

2.3.1. First line of defence (prevention)

As defined in Sub-chapter 3.1, the second level of defence in depth involves detecting and correcting the effects of deviations from normal operation and the effects of systems failures. For that purpose the following are implemented in normal operation:

- core and RCP [RCS] automatic control functions;"
- monitoring of limiting conditions of operation (LCOs)
- automatic limitation functions for core and RCP [RCS] parameters.

The core and reactor control functions implement corrective action by activation of safety or nonsafety systems whenever a perturbed situation is detected. For example, in the following actions could be implemented:

- opening of the Main Steam Bypass GCT [MSB] following a secondary pressure disturbance;
- triggering of the pressuriser spray system or the pressuriser heaters following a primary pressure disturbance;
- house-load operation following a loss of external power supply;

Additionally, LCO surveillance functions are implemented. An LCO surveillance function indicates or limits the variation of a process parameter such that the initial conditions of operation at the onset of a postulated initiating event are maintained as pre-supposed in the safety analyses. The LCO therefore bounds the operating range.

After exceeding the LCO, an alarm is displayed and automatic "passive" countermeasures that do not induce a power decrease are actuated (blockage of rod withdrawal, blockage of turbine load increase ...). In case these passive countermeasures and the operator actions that follow the alarm display do not enable the restoration of the authorised operating condition, automatic "active" countermeasures are actuated (partial trip¹, dilution stop, turbine load reduction ...).

These countermeasures are actuated with a time delay to allow fast operating transients, such as power level steps and load rejections, to succeed.

The analysis of design basis events does not take into account the beneficial aspects of functions ensured by systems involved in the preventive line (as they are generally not safety classified for that purpose).

¹ Fast power reduction achieved by the dropping of a certain number of RCCAs and consistently adjusting the turbine setpoint to reduce generator power on secondary side



PAGE : 7 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

2.3.2. Main defence line (protection)

UK EPR

If the effect of systems comprising the preventive line is insufficient to control the deviation, and to return the core to safe conditions, a Reactor Trip (RT) is initiated by the Protection System (RPR [PS]) [Ref-1] and engineered safety systems may be actuated.

As defined in Sub-chapter 3.2, three physical states are defined corresponding to shutdown conditions to be attained in design basis events (PCC) and RRC-A sequences.

These make it possible to establish a hierarchy of the functions used to attain shutdown conditions:

- controlled state: the core is subcritical (a return to short-term criticality before operator actions leading simply to low nuclear power may acceptable on a case by case basis for a few events), heat removal is assured on a short-term basis, for example via steam generators, core water inventory is stable, radioactive discharges remain acceptable,
- **safe shutdown state**: the core is subcritical, residual heat is being removed on a long-term basis, radioactive discharges remain acceptable,
- **final state**: the core is subcritical, residual heat is being removed via primary or secondary systems, radioactive discharges remain acceptable.

Note that controlled and safe shutdown states are applicable to PCC conditions while the final state is used only in RRC-A analyses.

As a general rule for the design basis events, only the action of safety classified systems is assumed when demonstrating compliance with the PCC or RRC-A acceptance criteria as indicated in the criteria for Structure, Systems and Components classification provided in Sub-chapter 3.2.

In order to introduce redundancy within the line of protection, the RPR [PS] is divided into two sub-systems, A and B.

For reactor trip signals processed in the RPR [PS], the following design rules are applied:

- for any PCC-2 condition which initiates an RT, if the main initiation signal is processed in one sub-system, a second initiating signal is processed in the opposite sub-system²,
- a sensor used for a main initiation signal for RT in a sub-system cannot be used by the second initiating signal in the opposite sub-system.

It may be necessary to inhibit an automatic signal to cancel actions initiated by the signal, for example to shut down a pump after automatic start-up by the RPR [PS]. This can be done by resetting or by using permissives.

² With the exception of the partial loss of core coolant flow where no additional RT is required.

SUB-CHAPTER : 14.7

PAGE : 8 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

A reset is an operator action to clear the memory of a stored automatic signal. In most cases, a reset does not imply any automatic action but only allows manual control of the system. For actuators that receive commands from the protection system, these commands have priority over post-accident manual actions. In this case, the reset of the protection system command is necessary to allow manual operation of the actuators in the control room in a post-accident situation on the safe path. In some specific cases, a permissive instead of a reset is used to inhibit signals coming from the protection system. A description of resets is given in section 3.5 of this sub-chapter.

Permissives can also be introduced to authorise the activation or deactivation of certain protection signals depending on the current status of the reactor. A permissive is a condition to be satisfied, based on the information given by a set of sensors. A permissive is produced as soon as its associated condition is satisfied.

There are two types of permissives, depending on whether the associated actions are performed automatically or manually:

- if the permissive is of the "automatic action" type, its validation (or invalidation) leads to automatic performance of the related actions,
- if the permissive is of the "manual action" type, its validation (or invalidation) does not lead to any automatic action, but allows the operator to perform the related actions manually.

A given permissive can be of the manual type with respect to activation, and of the automatic type with respect to deactivation, or vice versa.

Permissive signals have the same safety classification as the protective actions they inhibit. A description of permissives is given in section 3.6 of this sub-chapter.

2.3.3. Back-up line of defence

UK EPR

In accordance with the defence in depth principles and the HSE SAPs (notably FA.15), additional safety measures are introduced that aim to further reduce the risk of core melt, which could be caused typically by multiple failures such as total loss of a safeguard system.

To achieve such goal, the approach adopted is to ensure that a diverse means can be used as a back-up whenever the total failure of a safeguard system induces a significant risk of core melt. The event sequences that fall into this category are identified by Probabilistic Safety Assessment. Depending on the type of sequence, the diverse system may be another, already existing system, or an additional system specifically introduced to prevent the risk of core melt. For the additional systems, due to the low probability of the event sequences considered, it is acceptable to apply less stringent design requirements than for the normal safeguard systems and a safety classification consistent with the principles described in Sub-chapter 3.2 is adopted.

The deterministic analysis of the Risk Reduction Category A (RRC-A) event sequences provides the basis for the specification of the required characteristics and performance of the diverse systems.

Diversity can be provided between the trains of a redundant system or by another system, diverse from the system it has to back up. Both solutions are adopted for the EPR. Safety systems and functions have been designed applying functional diversity: the intention is to provide, whenever possible, a diverse system which can perform the desired function and bring the plant back to a safe condition in the highly unlikely event of all the redundant trains of a system becoming totally unavailable.

UK EPR

SUB-CHAPTER : 14.7

PAGE : 9 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

For frequent events (PCC-2) for which no back-up line has been identified, arguments are given in Sub-chapter 14.7 – Table 1 for why this situation is still acceptable from a safety point of view.

PAGE : 10 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

3. PROTECTION SYSTEM I&C ARCHITECTURE

This section describes the basic architecture of the I&C systems used to actuate the EPR control and protection functions, and explains the principles used to define protection system settings, and to modify or deactivate settings during changes in the reactor state.

3.1. SAFETY FUNCTIONS

UK EPR

To structure the Primary/Secondary (P/S) I&C functions, a hierarchy is used.

It is based on the objective of preventing or minimising the release of radioactivity to the environment during transients, by ensuring the integrity of the three barriers:

- the fuel cladding;
- the reactor coolant system;
- the containment.

The safety functions to be achieved to ensure a safe control of the plant can be divided into the five following basic safety functions or "control modes" [Ref-1].

- Reactivity control;
- Reactor heat removal;
- RCP [RCS] integrity;
- RCP [RCS] inventory control;
- Containment of radioactivity.

3.2. TYPES OF I&C FUNCTIONS

The I&C functions are divided into six hierarchical categories:

- Level 1 : Control I&C functions;
- Level 2 : Limiting Conditions of Operation (LCO) surveillance I&C functions;
- Level 3 : Limitations I&C functions;
- Level 4 : Protection I&C functions;
- Level 5 : Post Accident Management I&C functions;
- Level 6: RRC I&C functions.

PAGE : 11 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

3.2.1. Control I&C functions

UK EPR

The control I&C functions are those functions, which act on controlled parameters in order to follow control setpoints in all plant conditions.

Control I&C functions are Non-Classified (NC)

3.2.2. LCO surveillance I&C functions

The LCO surveillance I&C functions are those functions which are implemented to initiate (manually or automatically) in cases of violation of LCO. The functions contribute to maintaining the initial conditions within the limits adopted in the safety analyses.

3.2.3. Limitation I&C functions

The limitation I&C functions are functions which are implemented to initiate corrective measures (manually or automatically) in case the operating point comes too close to the protection system thresholds (avoidance of protection action).

The main objective of these functions is to improve the plant availability by terminating abnormal transients at an early stage in order to avoid actuation of a protection action.

The beneficial effect of limitation functions is not taken into account in safety analyses, under the rules applied in accident analysis. However credit for their role can be taken in probabilistic studies of certain transients.

3.2.4. Protection I&C functions

The protection I&C functions are functions which are implemented to mitigate the consequences of a Postulated Initiating Event (PIE) automatically after its detection. They include automatic actuation of protection actions and safety-grade systems, and automatic control of these actions during the short term accident phase. This phase is considered to last for 30 minutes after the occurrence of the first significant alarm following detection of the PIE.

The short term phase is the time period where the protection actions must be automatic. The EPR design is that automation of the protection actions should enable the controlled state to be reached after an accident, and to be maintained as long as it is required for safety purposes. Therefore there is no reliance on operator action to bring the plant to a safe stable state, manual actions being required to transfer the plant from the controlled state to the safe shutdown state.

The above requirements ensure automation of protection functions in the short term postaccident phase, but do not mean that beneficial operator actions are precluded: beneficial manual actions either to anticipate automatic actions, or to improve the mitigation level, are desirable, and these are permitted when they are in accordance with emergency operating guidelines.

3.2.5. Post accident management I&C functions

The post-accident I&C functions are the functions required to bring the plant from the controlled state to the safe shutdown state and to maintain it.

In the safety analyses, a manual action from the main control room cannot be credited within the 30 minutes after the first significant information given to the operator.

PAGE : 12 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

Thus, if actions to bring the plant to the safe shutdown have to be undertaken before 30 minutes, the required post-accident I&C functions must be automatic. Otherwise, manual post-accident functions are considered sufficient..

3.2.6. RRC I&C functions

UK EPR

The RRC I&C functions are those functions, which are implemented to mitigate the consequences of an RRC event (an RRC event could be either a PIE combined with a common cause failure or an event involving multiple coincident PIEs). The RRC I&C functions include either manual or automatic actuation of reactor trip and/or the safeguard systems, the control of these actions, or the simple detection of an accident which requires manual intervention from the operator more than 30 minutes after the first significant alarm.

3.3. BASIS FOR THE DEFINITION OF AN I&C FUNCTION

The concept of I&C functions is used to structure I&C tasks into small functional units such that each unit:

- gives a complete representation of a functional objective (safety objective or operational objective);
- can be classified according to its degree of safety importance;
- comprises the smallest entity form sensor to actuator to achieve its functional objective;
- is as far as possible independent from other units and therefore easily exchangeable.

The full set of I&C functions provides a modular functional structure for the I&C which forms the basis of the overall I&C architecture and enables process engineers to verify whether the postulated events are controlled and mitigated in the expected manner.

An I&C function must be as simple as possible.

It must rely on parameters as close as possible to:

- the physical phenomenon under control,
- a symptom-based approach.

An I&C function must rely on an event-based approach, when required.

An I&C function must be designed to avoid Non-unequivocally Safety Oriented (NUSO) I&C functions as far as possible. The NUSO definition is given in section 3.4.1

SUB-CHAPTER : 14.7

PAGE : 13 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

3.4. SET OF I&C FUNCTIONS

3.4.1. NUSO functions

UK EPR

When two I&C functions, with the same classification, perform opposing actions within the same safety system, the one which has priority over the other one is called Non-unequivocally Safety Oriented (NUSO). All other I&C functions are called Unequivocally Safety Oriented (USO).

The faulty actuation of NUSO, during many events, significantly lessens or impairs the actual plant safety level, because it prevents from the action of an other I&C function which is needed to mitigate the accident.

Due to their potential negative impact on safety when spuriously actuated, the NUSO I&C functions shall be designed in a way to minimise the probability of spurious action.

3.4.2. Setpoints scales

Setpoints result from the hierarchical organisation of I&C functions described above.

The overall I&C design approach to ensure a high level of plant safety is based on:

- consideration of the channel accuracy,
- consideration of the response time of the I&C function,
- the threshold margin to ensure plant reliability in case of failure of the dedicated I&C function,
- application of the single failure criterion to I&C systems,
- priority requirements between different I&C functions.

In Sub-chapter 14.7 - Figures 1 and 2, examples of setpoint scales with the corresponding actions are shown.

3.5. RESET OF AUTOMATIC PROTECTION FUNCTIONS

3.5.1. Definition

A reset is an operator action to clear the memory of a stored automatic signal. It may be necessary to inhibit an automatic signal to cancel actions initiated by the signal. In most cases, a reset does not imply any automatic action but only allows a manual control of the system. When actuators receive commands from the protection system, these commands have priority over manual actions. In this case, the reset of the protection system command is necessary to allow manual operation of the actuators in the control room in a post-accident situation on the safe path.

<u>Note</u>

As mentioned above, in general there is priority of automatic commands generated in PS over manual commands performed by the operator.

SUB-CHAPTER : 14.7

PAGE : 14 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

Most memories used are of two types:

- "reset priority" memories, for which the reset inhibits a signal if the conditions that govern signal activation are met at the time of actuation of the reset.
- "priority set" memories, for which the reset does not inhibit the signal, but inhibits storage of the signal if the conditions that determine signal activation are not met at the time of actuation of the reset.

3.5.2. Principles

UK EPR

Reset requirements with respect to protection system commands are defined in accordance with two basic hypotheses:

- the protection system issues non-reversible commands. This means that an initiated action is not ended even if the initiating conditions are no longer present.
- signals originated from the protection system are not stored as routine. Conditions for storage have to be defined individually for each signal.

3.5.3. Reset description

Resets (and associated memories) are analysed with respect to two types of initiating signals:

• Non-spurious commands

A reset must be configured only if the protection command is stored, since it must be possible to cancel the protection system command to return to normal operation once the required conditions are met. This reset will be of the non-priority type, except in special cases.

• Spurious commands.

There are two kinds of spurious commands: pulse-type and permanent: the approach for the first kind of command is the same as for non-spurious commands and permanent ones have a very low probability.

The concept of single failure is incorporated into the design of resets required on the safe path in a post-accident situation.

A 2 fold redundancy is chosen for resets that are configured for actions on the safe path in a post-accident situation. No redundancy is necessary for resets that are configured for actions not on the safe path in a post-accident situation (except in special cases).

In some specific cases, a permissive instead of a reset is used to inhibit signals coming from the protection system.

PAGE : 15 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

3.6. PERMISSIVE SIGNALS

3.6.1. Definitions

UK EPR

Permissives are introduced to authorise the activation or deactivation of certain protection signals, according to the current operating status of the plant unit. Consequently, certain manual or automatic actions, related to the permissive, are authorised or not.

As these deactivations are detrimental to safety when the reactor is at power, they are authorised only in certain conditions, called permissives.

Each permissive is associated with a key. The permissive corresponds to the condition to be satisfied, and the key launches the actions authorised by the permissive. There are two types of permissives, depending on whether the key triggers automatic or manual actions. A given permissive can be of the manual type with respect to activation, and be automatic with respect to deactivation, or vice versa.

Permissives are identified by the letter P followed by a suffix. Permissives related to PS protection functions are for example: P12, P14, P15... Keys are identified by the word KEY (upper cases) followed by the same suffix as the associated permissive (e.g. KEY12 for P12).

3.6.2. Principles

It must be possible to perform the actions associated with the permissives in normal operating conditions and in post-accident phases. Therefore, validation of permissives and KEY actuation by the operator is possible from both the PICS (Process Information and Control System) and the SICS (Safety Information and Control System). The PICS and SICS are the systems which allow the display of information from the different I&C automation systems in the main control room.

3.6.3. Permissive list

Examination of permissive requirements with respect to P/S related protection functions has led to definition of the following list (non exhaustive):

NAME	USE
P12	Inhibition of signals for return to cold shutdown
P13	Inhibition of signals for draining or filling of SGs during cold shutdown
P14	Authorisation to connect LHSI in RHR mode
P15	Activation of loop level protection
P16	Authorisation to switch RIS [SIS] cold to hot leg injection
P17	Activation of cold overpressure protection
P18	Authorisation to open transfer blowdown lines between SG
P19	Authorisation to perform secondary depressurisation

PAGE : 16 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

4. ADEQUACY OF DESIGN TO PROTECT THE PLANT AGAINST FAULTS – ALARP DISCUSSION

4.1. OVERVIEW OF PLANT PROTECTION

As described in section 2, several lines of defence are implemented in the design of the EPR. Deterministic protection aims at preventing any core damage and limits the radioactive release outside the containment. The main line of defence is designed on the basis of the fault studies in Sub-chapters 14.3 to 14.5. The overview of plant protection is then provided in the fault and protection schedule.

4.2. ANALYSIS OF FUNCTIONAL DIVERSITY

In order to ensure a high level of plant safety, the main line of defence is completed by a diverse line of protection which results from the RRC-A approach and the functional diversity analyses presented in Sub-chapters 16.1 and 16.5. These analyses ensure that two diverse lines of protection are sufficient to protect the plant for each frequent fault considered in the fault studies in Sub-chapters 14.3 and 14.4.

The results of these functional analyses are also provided in the fault and protection schedule.

4.3. RADIOLOGICAL CONSEQUENCES

The radiological consequences study presented in Sub-chapter 14.6 allows comparison with the SAP requirements. It demonstrates the adequacy of the design to protect the environment and people from radiation exposure consistent with the UK regulations for effective dose.

In addition to these studies, a Probabilistic Safety Assessment of the radiological releases and consequences allows an assessment of the plant protection by comparing the resulting doses and the frequency of releases (Sub-chapter 15.5). Demonstration, using a PSA model, that the nuclear safety risk from an EPR meets the BSO risk targets is considered to be an important element in the overall demonstration that the ALARP principle is met by the EPR (see Sub-chapter 17.4).

UK EPR

SUB-CHAPTER : 14.7

PAGE : 17 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

5. CONCLUSION

UK EPR

The safety measures described in this sub-chapter are illustrated and detailed for each transient considered in the fault schedule. This fault schedule illustrates that the plant is protected by two diverse lines of protection for the most frequent events as detailed in the analyses of functional diversity provided in Sub-chapter 16.5. The efficiency of the plant to protect people and the environment from radiation exposure is highlighted in the deterministic radiological consequences analyses provided in Sub-chapter 14.6 and the probabilistic analyses provided in Sub-chapter 15.5. These two contributions form an important element in the demonstration that the ALARP principle is met by the UK EPR.

PAGE : 18 / 58

PRE-CONSTRUCTION SAFETY REPORT

UK EPR

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (1/29)

			Input to o	lassifica	tion				SAFETY FUNCTIO	N		MAIN	LINE						DIV	ERSE LINI				
		R	eferences			Trans	ient ph	ases	Plant Level Safety Function		Lower Level Safety Function		Safety Functional	Groups			Lower Lovel Safety Function		Safery Functional G	roups				
descript	tion	ategory	Frequency	PCSR	Main Safety Function	Cont.	Safe	Final	Based on EPR process and international practice for PWR	Safety Cat.	Combination of the Plant Level Safety Function and the conditions of operations (normal, incident, accident)		ltem	Safety class	System Req.		Combination of the Plant Level Safety Function and the conditions of operations		hem	Sofety class			Supporting study	
3 Decrease				Ker.		state	state	state									(normal, inclutant, accident)							
												React	or trip - auto					Emergency the co	boron injection into re - diversified					
						x			Shutdown and maintain core sub-criticality	A	Negative reactivity fast insettion	Actuation	(1) - Low-low loop flow rate in one loop (2) - Low RCP speed in 2/4 loops Low Loop Flow Rate in 2 of 4 loops	Class 1	F1A	PS	High concentrated and high pressure boron injection	Actuation	ATWS signal (N-3 rod drop)	Class 2	F2	PS	ATWS LOOP covers	
					Reactivity							Front. Syst.	CRDM					Front. Syst.	EBS	-				
					Control							Tronc of or	- Choin				Negative reactivity fast insertion	Read Actuation	tor trip - auto Low RCP speed	Class 2	F2	SAS		E
(1) - Par loss of c coolant f (loss of c RCP)	ore f>1 flow one	PCC-2 10-2/(r.y)	1 - 5.9.10-2	1 - 14.3.8								Tu Actuation	rbine Trip RT checkback Turbine admission	Class 1	F1A	PS	II MAN NAM	Front. Syst. M Actuation	CRDM SIV closure SG P	Class 1	F1A	PS	Excessive increase in steam flow study	,
						x			Prevention of uncontrolled positive reactivity insertion into the core	A	RCS overcooling protection	Front. Syst.	valves				RCS overcooling protection	Front. Syst.	MSIV					+
(2) - For	ced								into the core			Actuation	RT checkback Full load MFW	Class 1	F1A	PS		Actuation	RT checkback	Class 2	F2	SAS	SAS order in case of ATWS following Pa failure	5
decrease reacto	or 👘	PCC-3 10- r.y) <f<10-< td=""><td>2</td><td>2 -</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Front. Syst.</td><td>isolation valves</td><td></td><td></td><td></td><td></td><td></td><td>isolation valves</td><td></td><td></td><td></td><td></td><td>+</td></f<10-<>	2	2 -								Front. Syst.	isolation valves						isolation valves					+
(4 pump		2/(r.y)		14.4.9		×			Transfer heat from the		Heat removal by Steam	Actuation Front. Syst.	SG P MSRT tion (1 train) + SG	Class 1	F1A	PS	Heat removal by Low Head	Actuation Front. Syst.	Charge line Manual PDS NS] in cold leg	Class 2	F2	SAS	Sequences of primary bleed and feed	
					Heat removal	x			reactor coolant to the ultimate heat sink	A	Generators - Emergency shutdown mode	Blowd Actuation Front. Syst.	own Isolation SG L EFWS injection lines & storages	Class 1	F1A	PS	Emergency Core Cooling System (ECCS)	Actuation Front. Syst.	Manual	Class 2	F1B	SAS	detailed in case of Total Loss Of FeedWater RRC-A	
													into a statuges					RCF Activ. & Elec Front. Syst.		Class 2	F1B	SAS		
					Other	x			Prevent the failure or limit the consequences of failure of a structure, system or component whose failure	A	Essential component protection	Overpres Actuation	ssure Control - ssure protection SG P	Class 1	F1A	PS	Essential component protection	SG safet Actuation	y valves opening Passi∨e	Class 1	F1A		Secondary overpressure studies of Sub chapter 3.4.1.5 illustrate	-
PERATIONS						x			could cause the impairment Shutdown and maintain core sub-criticality	A	Negative reactivity fast insertion	Actuation	MSRT or trip - auto Low-low loop flow rate in one loop	Class 1	F1A	PS		Front. Syst.	MSSV				I	T
POWER O					Reactivity Control							Actuation	CRDM rbine Trip RT checkback Turbine admission	Class 1	F1A	PS								
Reacto coolar Pump sei	nt			14.5.8		×			Prevention of uncontrolled positive reactivity insertion into the core	A	RCS overcooling protection	Actuation	valves FW isolation (4SG) RT checkback Full load MFW	Class 1	F1A	PS								
(blocke rotor) &) 6/(r	PCC-4 10- r.y) <f<10- 4/(r.y)</f<10- 	-			x						Actuation	isolation valves e Control - Cooling SG P	Class 1	F1A	PS		N/A - d	iversity is applied to fr	equent initi	iating ever	nt above 1	0 ⁻³ /r.y	
Reacto coolant p shaft bro	ump			14.5.9	Heat removal	x			Transfer heat from the reactor coolant to the ultimate heat sink	A	Heat removal by Steam Generators - Emergency shutdown mode	Blowd Actuation	tion (1 train) + SG own Isolation	Class 1	F1A	PS								
					Other	x			Prevent the failure or limit the consequences of failure of a structure, system or	A	Essential component protection	Overpres Actuation	lines & storages sure Control - sure protection SG P	Class 1	F1A	PS								
					Confinement	x			component whose failure Maintain integrity of the Reactor Coolant Pressure Boundary	A	RCS overpressure protection	Front. Syst. Hot overpr Actuation Front. Syst.	MSRT essure protection Passive PSV	Class 1	F1A	•								
					Reactivity Control		x		Shutdown and maintain core sub-criticality	в	Compensation for shutdown moderator effect	Emergency	boron injection into ore - Manual Manual	Class 2	F1B	SAS								
Emerger Operati	ng	All	N/A	All			x			в	Heat removal by Steam Generators - Emergency shutdown mode		e Control - Cooling Manual	Class 2	F1B	SAS			ē	Appendix				In hav
Procedu		~"	NFA	~	Heat removal				Transfer heat from the reactor coolant to the	в		RCS depres	ssurisation by PZR ety valves	Class 2	F1B	SAS			See	Appendix /	~			
									ultimate heat sink	5	Heat removal in shutdown mode by Residual Heat Removal system (RHRS)	Activ. & Elec Front. Syst. RHR connect	Manual PSV ion and start-up (no			040								
							×			В		Activ. & Elec Front. Syst.	l signal) Manual RHRS	Class 2	F1B	SAS								

Reactor coolant pump shaft break consequences bounded by Reactor Coolant Pump seizure (locked rotor)

In case of Shaft break, the possibility to have a LOCA is managed by the actuation of MHSI by the operator. This manual actuation is Class 2

PAGE : 19 / 58

PRE-CONSTRUCTION SAFETY REPORT

UK EPR

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (2/29)

			Input to c	lassifica	lion			SAFETY FUNCTION	DN		MAIN	LINE						ON	TERSE LIN	E			
No.	Fault	1	References		Main Safety	Tran	siont phas	Puricuon	Safety Cat.	Lower Level Safety Function Combination of the Plant		Safety Functional	Groups			Lower Level Befory Purchase Combination of the Plant		Beley Punctional C				Supporting and	Comments
	description		Frequency	PCSR Ref.	Function		Safe F state st			Lovel Safety Function and the conditions of operations (normal, incident, accident)		Item	Safety class	System Req.		Laval Subby Function and the conditions of operations (normal, incident, excident)		Bern	Safety class	Syst Req			
	eactivity power Uncontrolled RCCA bank withdrawal at power					×		Shutdown and maintain core sub-oriticality	A	Negative reactivity fast insertion	React Actuation Front. Syst.	or trip - auto DNBR (slowest transient) High NF rate of change (fastest transients) ORDM	Class 1	F1A	PS	High concentrated and high pressure boron injection	Emergency the or Actuation	ATWS signal (N-3 rod drop)	Class 2	F2	PS	ATWS cover	
	Uncontrolled RCCA bank thdrawal from HZP				Reactivity Control	×					FIGH. Syst.	CKDW				Negative reactivity fast insertion		tor trip - auto High AO High neutron flux HL P	Class 2	F2	SAS		
	RCCA misalignment p to rod drop Start-up of an	PCC-2 f≥10-2/(r.y)	- for all but 7.10-3 for CVCS	14.3.9 14.3.10 14.3.11		×		Prevention of uncontrolled	A	RCS overcooling protection		nbine Trip RT checkback Turbine admission valves	Class 1	F1A	PS			SIV closure SG P	Class 1	F1A	PS	Excessive increase in steam flow study	* for CVCS malfunction
i	active reactor oolant loop at an improper temperature	PCC-3	1.35.10-3 for single RCCA withdrawal	14.3.12		x		into the core		RUS overcooling protection		W isolation (4SG) RT checkback Full load MFW isolation valves	Class 1	F1A	PS	 RCS overcooling protection 	Actuation Front. Syst	Full load MFW isolation valves	Class 2	F2	SAS	SAS order in case of ATWS following PS failure	refer to the CVCS malfunc mode for main mitigativ diversity
t	CVCS malfunction lat results in a decrease in boron	20.97		14.4.13		×					Actuation Front. Syst.		Class 1	F1A	PS		di Actuation Front. Syst	PDS	Class 2	F2	SAS		
	oncentration n the reactor coolant *				Heat removal	x		Transfer heat from the reactor coolant to the ultimate heat sink	A	Heat removal by Steam Generators - Emergency shutdown mode	Actuation Front. Syst.	own Isolation	Class 1	F1A	PS	Heat removal by Low Head Emergency Core Cooling System (ECCS)	Actuation Front. Syst	MHSI + LHSI	Class 2	F1B	SAS	Sequences of primary bleed and feed detailed in case of Total Loss Of FeedWater RRC-A	
	single RCCA withdrawal					×											Activ. & Ele Front. Syst	e stop - Manu Manual RCP	Class 2	F1B	SAS		
					Other	x		Prevent the failure or limit the consequences of failure of a structure, system or component whose failure	A	Essential component protection		sure Control - sure protection SG P MSRT	Class 1	F1A	PS	Essential component protection	SG safe Actuation Front. Syst	Passive MSSV	Class 1	F1A	•	Secondary overpressure studies of Sub- chapter 3.4.1.5 illustrate	
PERATIONS	Inadvertent loading of a uel assembly n an improper position	PCC-3 10- 4/(r.y) <f<10- 2/(r.y)</f<10- 	2.10 ⁻³	14.4.8		N/A		If	the incorrect	fuel loading pattern is not detec	ted prior to pov	ver operations, it coul	d lead to a d	hange in the	e power dis	tribution predicted for the core (design and the	reby exceed the safe	y limits. De	etection m	ethods do	not fit in fault schedule format - see PCSR fo	r further details.
POWER OI						x		Shuldown and maintain core sub-criticality	A	Negative reactivity fast insertion	React Actuation Front. Syst.	or trip - auto High NF rate of change CRDM	Class 1	F1A	PS								
					Reactivity Control	×		Prevention of uncontrolled positive reactivity insertion	A	RCS overcooling protection	Actuation Front. Syst.	rbine Trip RT checkback Turbine admission valves	Class 1	F1A	PS								
	Spectrum of	PCC-4				x		into the core			Full load Mi Actuation Front. Syst.	W isolation (4SG) RT checkback Full load MFW isolation valves	Class 1	F1A	PS								
	CCA ejection accidents	10- 6/(r.y) <f<10- 4/(r.y)</f<10- 		14.5.5	Heat removal	×		Transfer heat from the reactor coolant to the	A	Heat removal by Steam Generators - Emergency	Actuation Front. Syst.		Class 1	F1A	PS	N/A - diversity	is applied to f	requent initiating even	t above 10	[∂] ir.y		N/A	
						×		utimate heat sink		shutdown mode	Blowd Actuation Front. Syst.	SG L EFWS injection lines & storages	Class 1	F1A	PS								
					Other	×		Prevent the failure or limit the consequences of failure of a structure, system or component whose failure	A	Essential component protection	Overpres Actuation Front. Syst.	MSRT	Class 1	F1A	PS								
					Confinement	×		Maintain integrity of the Reactor Coolant Pressure Boundary	^	RCS overpressure protection		Passive Passive PSV	Class 1	F1A	-								

nts

tion resulting in a incentration, please function in shutdown gative feature and sity

SUB-CHAPTER : 14.7

PAGE : 20 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (3/29)

		Input to	classificati	on			SAFETY FUNCTION	N		MAIN L	LINE				DWERSELINE
		References			Trans	sient phas	es Plant Level Safety Function		Lower Level Safety Function	[Safety Functional (Groups			Lower Level Bately Function Safety Functional Groups Comments
Fault description	Category	Frequency	PCSR Ref.	Main Safety Function	Cont. state	Safe F state s	Based on EPR process and international practice for PWR	Safety Cat	Combination of the Plant Level Safety Function and the conditions of operations (normal, incident, accident)		ltem	Safety class	System Req.		Sector Constants of the Part Land Sector Constants of spantanes (downall relation) doublers
Reactivity powe	r distribution							I							
			-			-				Front. Syst.		1			
				Reactivity Control		×	Shutdown and maintain core sub-criticality	в	Compensation for shutdown moderator effect		boron injection into ore - Manual Manual EBS	Class 2	FIB	SAS	
Emergency Operating	AB	NA	All			x	Transfer heat from the	В	Heat removal by Steam Generators - Emergency shutdown mode	Actuation Front. Syst. RCS depres	Manual MSRT	Class 2	F1B	SAS	have a LOCA is managed by the act
Procedure				Heat removal			reactor coolant to the ultimate heat sink	В	Heat removal in shutdown mode by Residual Heat Removal system (RHRS)	Activ. & Elec Front. Syst. RHR connect	Manual PSV tion and start-up (no	Class 2	F1B	SAS	
						×		в		Activ. & Elec Front. Syst.	Manual RHRS	Class 2	F1B	SAS	
malfunction	PCC2			Reactivity		x	N/A Prevention of uncontrolled		-	Anti-dik	ution isolation				Anti-dilution isolation diversified
at results in a decrease in	Þ10 ⁻ /(r.y)	7.10 ⁻³	14.3.13	Control			x positive reactivity insertion into the core	A .	Anti-dilution protection	Actuation Front. Syst.	Cb CVCS	Class 1	F1A	PS	Anti-dilution protection Actuation Manual Front. Syst. CVCS F2 SAS
rod cluster control assembly (RCCA) bank withdrawal (states B, C & D)	PCC3 10- 4/(r.y) <f<10- 2/(r.y)</f<10- 	.	14.4.12		N/A							A sp	ecific protec	tion functio	ction aims at making these scenarios impossible - it is no longer studied
										Actuation Front. Syst.	Alarm High NF rate of change PS	Class 1	FIA	PS	
oron dilution	PCC-4				×		Prevention of uncontrolled	A	Anti-dilution protection		Cb CVCS	Class 1	FIA	PS	N/A - diversity is applied to frequent initiating event above 10-3/r.y
ue to a non-	6/(r.y) <f<10-< td=""><td></td><td>14.5.12</td><td>Reactivity Control</td><td></td><td></td><td>positive reactivity insertion into the core</td><td></td><td>Anti-dilution protection</td><td>Isolation of H</td><td>IP cooler in case of (P RRI > P RCV)</td><td></td><td>F1B</td><td>SAS</td><td>Isolation of HP cooler in case of leak (P RRI < P RCV) is provided as defense-in-depth in some case of leak to limit high release of radioactivity liquid inside containement.</td></f<10-<>		14.5.12	Reactivity Control			positive reactivity insertion into the core		Anti-dilution protection	Isolation of H	IP cooler in case of (P RRI > P RCV)		F1B	SAS	Isolation of HP cooler in case of leak (P RRI < P RCV) is provided as defense-in-depth in some case of leak to limit high release of radioactivity liquid inside containement.
lable ruptur						×		в	Anti-aiution protection	Actuation	Manual	Class 2	PIB	SAS	information is not presented
lable ruptur of a heat changer tub tates B. C &										Front. Syst.	CVCS				
able ruptur of a heat hanger tub lates B. C &									Anti-dilution protection	Actuation Front, Syst.	of one RHR train Cb CVCS	Class 2	FIB	SAS	

UK EPR

SUB-CHAPTER : 14.7

PAGE : 21 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

UK EPR

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (4/29)

			Input to	classifica	tion				SAFETY FUNCTIO	N		MAIN LI	NE						DIVI	ERSE LIN	E			
No.			References				unsient j	phases	Plant Level Safety Function		Lower Level Safety Function	\$	Safety Functional G	roups			Lower Lovel Safety Function	9 	afety Functional G	roups		-		Comments
	Fault description		Frequenc	PCSR Ref.	Main Safety Function	Con	nt. Safe te state		Based on EPR process and international practice for PWR	Safety Cat.	Combination of the Plant Level Safety Function and the conditions of operations (normal, incident, accident)		ltem	Safety class			Combination of the Plant Level Stifely Function and the conditions of operations (normal, insident, accident)		ltem	Safety class	Syst Req.		Supporting study	
	crease in RCS	inventory										React	or trip - auto						oron injection into - diversified					
						×			Shutdown and maintain core sub-criticality	A	Negative reactivity fast insertion	Actuation	PZR L PZR P	Class 1	F1A	PS	High concentrated and high pressure boron injection	Actuation	ATWS signal (N-3 rod drop)	Class 2	F2	PS	ATWS cover	
												Front. Syst.	CRDM					Front. Syst.	EBS					
					Reactivity												Negative reactivity fast insertion	Reacto	r trip - auto HL P	Class 2	F2	SAS		
					Control												-	Front. Syst.	CRDM					
						×						Actuation	r <mark>bine Trip</mark> RT checkback	Class 1	F1A	PS	_	MSIV Actuation	/ closure SG P SG L	Class 1	F1A	PS	Excessive increase in steam flow study	These parts of transient are provided in case of isolation of charging line and seal
							_		Prevention of uncontrolled positive reactivity insertion into the core	А	RCS overcooling protection	Front. Syst.	Turbine admission valves				RCS overcooling protection	Front. Syst.	MSIV					injection would fail leading to PZR filling. Consequently, such information does not
	CVCS malfunction causing increase in	PCC-2 f>10-2/(r.y)	-	14.3.14		×							RT checkback Full load MFW isolation valves	Class 1	F1A	PS	-	Actuation Front. Syst.	RT checkback Full load MFW isolation valves	Class 2	F2	SAS	SAS order in case of ATWS following PS failure	fully belong to the main line of defense.
IONS	eactor coolant inventory					×	-					SG Pressure Actuation Front. Syst.	SG P	Class 1	F1A	PS	-	Opening of s Actuation Front. Syst.	Severe accident Manual PDS	Class 2	F2	SAS		
R OPERAT					Heat remove	ıl ×			Transfer heat from the reactor coolant to the ultimate heat sink	A	Heat removal by Steam Generators - Emergency shutdown mode		tion (1 train) + SG SG L EFWS injection	Class 1	F1A	PS	Heat removal by Low Head Emergency Core Cooling		in cold leg Manual MHSI + LHSI	Class 2	F1B	SAS	Sequences of primary bleed and feed detailed in case of Total Loss Of FeedWater RRC-A	
POWEI						×	+						lines & storages						top - Manu Manual RCP	Class 2	F1B	SAS		
					Other	×			Prevent the failure or limit the consequences of failure of a structure, system or	А	Essential component protection	Overpres Actuation	sure Control - sure protection SG P MSRT	Class 1	F1A	PS	Essential component protection	SG safety v Actuation	valves opening Passive MSSV	Class 1	F1A	-	Secondary overpressure studies of Sub- chapter 3.4.1.5 illustrate	
					Confinemen	×			component whose failure Maintain integrity of the Reactor Coolant Pressure	A	RCS overpressure protection	Actuation Front. Syst.	of charging line PZR L CVCS isolation valve	Class 1	F1A	PS	-	Activ. & Elec Front. Syst.	ssure protection Passive PSV	Class 1	F1A	-	Primary overpressure studies of Sub- chapter 3.4.1.5 illustrate	The isolation of charging line is the main line of defense in such transient
						×			Boundary			Actuation Front. Syst.	MCP seal injection PZR L CVCS isolation valve	Class 1	F1A	PS		Activ. & Elec Front. Syst.	ssure protection Passive PSV	Class 1	F1A	-		
					Reactivity Control		×		Shutdown and maintain core sub-criticality	В	Compensation for shutdown moderator effect		poron injection into pre - Manual Manual	Class 2	F1B	SAS	·							
	Emergency Operating Procedure				Heat remove	al	×		Transfer heat from the reactor coolant to the	В	Heat removal by Steam Generators - Emergency shutdown mode	Actuation Front. Syst.	e Control - Cooling Manual MSRT		F1B	SAS			See	Appendix	A			Normally, in such event there is no need to reach a safe shutdown state
							x		ultimate heat sink	В	Heat removal in shutdown mode by Residual Heat Removal system (RHRS)		ion and start-up (no I signal) Manual RHRS		F1B	SAS								

PAGE : 22 / 58

PRE-CONSTRUCTION SAFETY REPORT

UK EPR

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (5/29)

		Input to clas	ssificatior	n				SAFETY FUNCTION	I		MAIN L	INE						DIVE	ERSE LINE				
Fault	R	ferences		Main Safety	Tran	sient pha		Plant Level Safety Function	o	Lower Level Safety Function Combination of the Plant Level	[Safety Functional	Groups		C&I	Lower Level Safety Function Combination of the Plant Level		Safety Functional Gr	oups			Supporting study	Comments
description	Category	Frequency	PCSR Ref.	Function	Cont. state	Safe F state s	inal tate	Based on EPR process and international practice for PWR	Salety Cal	Safety Function and the conditions of operations (normal, incident, accident)		ltem	Safety class	System Req.	plationi	Solaty Function and the conditions of operations (normal, incident, accident)		ltom	Safety class	Syst Req.		aupporting study	
Decrease in RCS	water inventory										Reacto	or trip - auto						ooron injection into e - diversified					
					x		:	Shutdown and maintain core sub-criticality	A	Negative reactivity fast insertion		PZR L DNBR HL P	Class 1	F1A	PS	High concentrated and high pressure boron injection	Actuation	ATWS signal (N-3 rod drop)	Class 2	F2	PS	ATWS SB provided in technical report about diversity	Question remains about SB-LOCA with break on EBS (capacity of the EBS tanks).
											Front. Syst.	CRDM					Front. Syst. React	EBS					
				Reactivity Control			:	Shutdown and maintain core sub-criticality	A							Negative reactivity fast insertion	Actuation	HL P	Class 2	F2	SAS		
											Turi	bine Trip					Front. Syst.	CRDM V closure					
					x			Prevention of uncontrolled positive reactivity insertion	A	RCS overcooling protection	Actuation Front. Syst.	RT checkback Turbine admission valves	Class 1	F1A	PS	RCS overcooling protection	Actuation Front. Syst.	SG P MSIV	Class 1	F1A	PS	Excessive increase in steam flow study	
					x			into the core	~	Res overcooling protection		W isolation (4SG) RT checkback Full load MFW isolation valves	Class 1	F1A	PS	NCC Overcooling protection	Full load MI Actuation Front. Syst.	RT checkback Full load MFW isolation valves	Class 2	F2	SAS	SAS order in case of ATWS following PS failure	
CVCS malfunction causing	PCC-2				x						Auto	Control - Cooling - b (MSRT) SIS signal [PZR P]	Class 1	F1A	PS			Control - Cooling - Manu Manual	Class 2	F1B	SAS	CM2) WITH FAILURE OF THE PARTIAL COOL-DOWN SIGNAL (STATE A) - PCSR	A diversified way to control the SG pressure could use the fact that the 4 MSRTs are independent and that the PS is working or
decrease in reactor coolant inventory (state A)	f>10-2/(r.y)	7.10 ⁻³	14.3.14		x			Maintain sufficient Reactor Coolant System water	A	Water injection into the RCS	-	MSRT jection - Auto SIS signal [PZR P] MHSI	Class 1	F1A	PS	Water injection into the RCS	Front. Syst.	MSRT in cold leg Manual	Class 2	F1B	SAS	Sub-chapter 16.1.3.3.6 Covered by LOCA (BREAK SIZE UP TO 20 CM2) WITHOUT MHSI (STATE A) - PCSR	the manual opening of the MSRTs
								inventory for core cooling		Prevention of RCS drainage	Isolation of C	MHSI CVCS letdown line ion SI sequence)				Prevention of RCS drainage	Front. Syst.	LHSI				Sub-chapter 16.1.3.3.7	
				Heat removal	x				A	through auxiliary lines		SIS signal [PZR P] CVCS letdown valve	Class 1	F1A	PS	through auxiliary lines	Actuation Front. Syst.	Manual CVCS letdown valve	Class 2	F1B	SAS	-	
					x						Actuation Front. Syst.	MSRT	Class 1	F1A	PS		Opening o disc Actuation Front. Syst.	f severe accident harge line Manual PDS	Class 2	F2	SAS		
					x			ransfer heat from the reactor coolant to the ultimate heat sink	A	Heat removal by Steam Generators - Emergency shutdown mode	Blowdo Actuation	ion (1 train) + SG wn Isolation SG L EFWS injection lines	Class 1	F1A	PS	Heat removal by Low Head Emergency Core Cooling System (ECCS)	SIS [RI Actuation Front. Syst.	S] in cold leg Manual MHSI + LHSI	Class 2	F1B	SAS	Sequences of primary bleed and feed detailed in case of Total Loss Of FeedWater RRC-A	
					x						Tiont. Syst.	& storages						stop - Manu Manual RCP	Class 2	F1B	SAS		
				Other	x			consequences of failure of a structure, system or component whose failure	A	Essential component protection		sure Control - sure protection SG P MSRT	Class 1	F1A	PS	Essential component protection		valves opening Passive MSSV	Class 1	F1A	-	Secondary overpressure studies of Sub- chapter 3.4.1.5 illustrate	
				Confinement	x			Limit the release of radioactive material from the reactor containment	A	Containment building isolation	Containment	isolation stage 1 / SIS signal [PZR P] Containment isolation valves	Class 1	F1A	PS	No need for diversity in case o		tion - there is no direc	t release in	to the cont	ainment		
Inadvertent opening of a pressurizer safety valve	PCC-3 10 ⁻⁴ /(r.y) <f<10<sup>- ²/(r.y)</f<10<sup>	1.68.10 ⁻³	14.4.3		N/A										This tra	nsient is fully covered by the SB	LOCA in state A						

PAGE : 23 / 58

PRE-CONSTRUCTION SAFETY REPORT

UK EPR

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (6/29)

		Input to cla	ssification						ON		MAIN							DIVE	RSE LINE			
Fault	R	eferences		Main Safety	Trar	nsient pł	hases	Plant Level Safety Function		Lower Level Safety Function		Safety Functional (iroups		C&I platform	Lower Lovet Safety Function	Safety Pt	nctional Gro	aque			
description	Category	Frequency	PCSR Ref.	Function	Cont. state	. Safe state	Final state	Based on EPR process and international practice for PWR	Safety Cat.	Safety Function and the conditions of operations (normal, incident, accident)		Item	Safety class	System Req.	plationin	Salety Function and the conditions of operations (normal, incident, accident)	, i	em	Safety class	Syst Req.		Supporting
	water inventory										React	or trip - auto					Emergency boron inje the core - divers					
					x			Shutdown and maintain core sub-criticality	A	Negative reactivity fast insertion	Actuation	PZR P HL P	Class 1	F1A	PS	High concentrated and high pressure boron injection		S signal rod drop)	Class 2	F2	PS	ATWS c
											Front. Syst.	CRDM					Front. Syst. E	BS				
																	Reactor trip - a	uto				
				Reactivity Control	x			Shutdown and maintain core sub-criticality	A							Negative reactivity fast insertion	Actuation H	IL P	Class 2	F2	SAS	
											T	rbine Trip					Front. Syst. C	RDM				
					x			Prevention of uncontrolled			Actuation Front. Syst.		Class 1	F1A	PS		Actuation S	G P ISIV	Class 1	F1A	PS	Excessive increase in
Small break (not greater than					x			positive reactivity insertion into the core	A	RCS overcooling protection	Full load M Actuation Front. Syst.	FW isolation (4SG) RT checkback Full load MFW	Class 1	F1A	PS	RCS overcooling protection	Front Svet Full lo	eckback ad MFW	Class 2	F2	SAS	SAS order in case of A failure
DN50) including a break occuring on the	PCC-3 10 ⁻⁴ /(r.y) <f<10<sup>-</f<10<sup>	6.10 ⁻⁴	14.4.5		x						SG Pressure	isolation valves Control - Cooling - to (MSRT)	Class 1	F1A	PS		SG Pressure Control - Manu	Cooling -	Class 2	F1B	SAS	Covered by LOCA (BRE CM2) WITH FAILURE
Extra Boration System	²/(r.y)								A	Water injection into the RCS	Front. Syst.					Water injection into the RCS	Front. Syst. M	anual SRT				COOL-DOWN SIGNAL Sub-chapter 1 Covered by LOCA (BRE
injection line (State A)					x			Maintain sufficient Reactor Coolant System water inventory for core cooling				njection - Auto SIS signal [PZR P] MHSI	Class 1	F1A	PS			anual HSI	Class 2	F1B	SAS	Covered by LOCA (BRE CM2) WITHOUT MHSI Sub-chapter 1
					x				A	Prevention of RCS drainage through auxiliary lines	(RCS isola	CVCS letdown line tion SI sequence)	Class 1	F1A	PS	Prevention of RCS drainage through auxiliary lines	Isolation of CVCS lete		Class 2	F1B	SAS	-
				Heat removal						through auxiliary lines	Front. Syst.	SIS signal [PZR P] CVCS letdown valve				unough auxiliary intes		anual down valve				
					x						Actuation Front. Syst.	e Control - Cooling SG P MSRT	Class 1	F1A	PS		Front. Syst. F	anual PDS	Class 2	F2	SAS	
					x			Transfer heat from the reactor coolant to the ultimate heat sink	A	Heat removal by Steam Generators - Emergency shutdown mode	EFW actua Actuation Front. Syst.	tion (1 train) + SG SG L EFWS injection lines	Class 1	F1A	PS	Heat removal by Low Head Emergency Core Cooling System (ECCS)		l leg anual I + LHSI	Class 2	F1B	SAS	Sequences of primar detailed in case of Total RRC-
					x							& storages					RCP stop - Ma Activ. & Elec Ma		Class 2	F1B	SAS	
				Other	x			Prevent the failure or limit the consequences of failure of a structure, system or		Essential component protection		SSURE Control - SG P MSRT	Class 1	F1A	PS	Essential component protection	SG safety valves o Actuation Pa		Class 1	F1A	-	Secondary overpressu chapter 3.4.1.5
				Confinement	x			Limit the release of radioactive material from the reactor containment	A	Containment building isolation	Containmen	t isolation stage 1 / SIS signal [PZR P] Containment	Class 1	F1A	PS	Containment building isolation	Containment isol Actuation Ma Front Supt	ation anual ainment	Class 2	F1B	SAS	
Loss of primary coolant outside the containment	PCC-3 10-4/(r.y) <f<10- 2/(r.y)</f<10- 	-	14.4.11	Confinement	x			Limitation of radioactive release outside containment from radioactive auxiliary systems	A	Due to the		isolation valves	chedule do	es not preser	nt them. The	e leaks are terminated after dete	ISOlatio	on valves Iding or Nucle	ear Auxiliar	y Building	s. The ope	erator isolates the corresp

ing storiy	Comments
S cover	Question remains about SB-LOCA with break on EBS (capacity of the EBS tanks).
e in steam flow study	
of ATWS following PS lure	
RE OF THE PARTIAL AL (STATE A) - PCSR er 16.1.3.3.6	A diversified way to control the SG pressure could use the fact that the 4 MSRTs are independent and that the PS is working or the manual opening of the MSRTs
REAK SIZE UP TO 20 ISI (STATE A) - PCSR er 16.1.3.3.7	
-	
nary bleed and feed tal Loss Of FeedWater IC-A	
ssure studies of Sub- .1.5 illustrate	
	Containment isolation stage 2 is not considered since the containment pressure does not increase sufficiently
esponding pipes from th	ne Main Control Room.

SUB-CHAPTER : 14.7

PAGE : 24 / 58

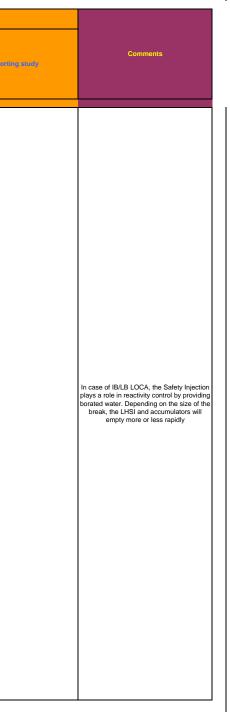
CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (7/29)

		Input to cla	ssificatio	n					ОМ		MAIN	LINE					OIVERSE LINE	
								Plant Level Safety Function		Lower Level Safety Function		Safety Functional	Groups			Lower Level Safety Function	Safety Functional Groups	
Fault description	Category	eferences Frequency	PCSR Ref.	Main Safety Function	Cont. state	nsient pł . Safe e state	Final	Based on EPR process and international practice for PWR	Safety Cat.	Combination of the Plant Level Safety Function and the conditions of operations (normal, incident, accident)		ltem	Safety class	System Req.	C&I platform	Combination of the Plant Level Safety Function and the conditions of operations (normal, insident, acaident)	Room district digest Room	Suppor
Decrease in RC	S water inventory				x			Shutdown and maintain core sub-criticality	A	Negative reactivity fast insertion	Actuation	tor trip - auto PZR P HL P CRDM	Class 1	F1A	PS			
				Reactivity Control	x			Prevention of uncontrolled			Front. Syst. Actuation Front. Syst.	RT checkback Turbine admission	Class 1	F1A	PS			
					x			positive reactivity insertion into the core	A	RCS overcooling protection		valves FW isolation (4SG) RT checkback Full load MFW isolation valves	Class 1	F1A	PS			
												e Control - Cooling - tto (MSRT) SIS signal [PZR P]	Class 1	F1A	PS			
											Actuation Front. Syst.	njection - Auto SIS signal [PZR P] MHSI	Class 1	F1A	PS			
					x				A	Water injection into the RCS	Colle Actuation Front. Syst.	IRWST systems	Class 1	F1A	PS			
								Maintain sufficient Reactor Coolant System water inventory for core cooling			Actuation Front. Syst.	VST cooling Passive IRWST systems on in cold leg - Auto	Class 1	F1A	PS			
Intermediate and large breal	5 700 /	6.10 ⁻⁴ (20-45cm²)		Heat removal							Front. Syst.	SIS signal [PZR P] LHSI Jlators injection Passive	Class 1 Class 1	F1A F1A	PS PS			
LOCA (up to the surge linebreak in states A and B)	(10-6/(r.y) <r<10-< td=""><td>1.6.10⁻⁵ (45-180cm²) 1.3.10⁻⁶ (180-830cm²)</td><td></td><td></td><td>x</td><td></td><td></td><td>-</td><td>A</td><td>Prevention of RCS drainage through auxiliary lines</td><td>(RCS isola</td><td>Accumulators CVCS letdown line ation SI sequence) SIS signal [PZR P]</td><td>Class 1</td><td>F1A</td><td>PS</td><td></td><td>$N\!/A$ - diversity is applied to frequent initiating event above 10-3/r.y</td><td></td></r<10-<>	1.6.10 ⁻⁵ (45-180cm ²) 1.3.10 ⁻⁶ (180-830cm ²)			x			-	A	Prevention of RCS drainage through auxiliary lines	(RCS isola	Accumulators CVCS letdown line ation SI sequence) SIS signal [PZR P]	Class 1	F1A	PS		$N\!/A$ - diversity is applied to frequent initiating event above 10-3/r.y	
		, , ,									Front. Syst.	CVCS letdown valve						
					x			Transfer heat from the reactor coolant to the ultimate heat sink	A	Heat removal by Steam Generators - Emergency shutdown mode	Actuation Front. Syst. EFW actua Blowd Actuation	ation (1 train) + SG	Class 1	F1A	PS			
					x			Prevent the failure or limit the			Front. Syst.	EFWS injection lines & storages ssure Control - ssure protection	Class 1	F1A	PS			
				Other	x			consequences of failure of a structure, system or component whose failure could cause the impairment of	A	Essential component protection	RCP	SG P MSRT Stop - Auto DP over RCP + SIS	Class 1 Class 1	F1A F1A	PS PS			
								a safety function			Actuation Front. Syst. Containmen RCF	signal RCP nt isolation stage 1 / PB isolation						
				Confinement	x			Limit the release of radioactive material from the	A	Containment building isolation	Actuation Front. Syst.	SIS [PZR P] Passive Containment isolation valves	Class 1	F1A	PS			
								reactor containment				nt isolation stage 2 SIS signal [PZR P] Containment isolation valves	Class 1	F1A	PS			

UK EPR



PAGE : 25 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

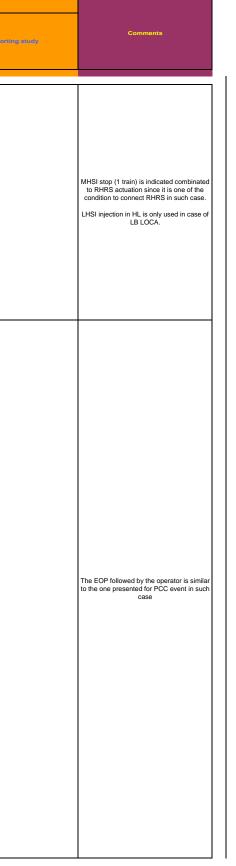
PRE-CONSTRUCTION SAFETY REPORT

UK EPR

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (8/29)

			Input to cla	ssificatio	1		SAFETY FUNCT			MAIN LINE				
						_	Ses Plant Level Safety Function		Lower Level Safety Function	Safety Functional C	Groups			Lower Level Safety Function Safety Functional Groups
des	Fault scription	R	References	PCSR Ref.	Main Safety Function	Transient phas Cont. Safe F state state s	Based on EPR process and international practice for PWR		Combination of the Plant Level Safety Function and the conditions of operations (normal, incident, accident)	Item	Safety class	System Req.	C&I platform	Combination of this Plant Land Solary Function and the condition of (minutions (month, assister), besident)
Decre	ease in RCS	water inventory												
					Reactivity Control	x	Shutdown and maintain core sub-criticality	в	Compensation for shutdown moderator effect	Emergency boron injection into the core - Manual Actuation Manual	Class 2	F1B	SAS	
						x	Maintain sufficient Reactor Coolant System water inventory for core cooling	в	Water injection into the RCS	Front. Syst. EBS LHSI injection in HL Actuation Manual	Class 2	F1B	SAS	
						x		В	Heat removal by Steam Generators - Emergency	Front. Syst. LHSI SG Pressure Control - Cooling Actuation Manual	Class 2	F1B	SAS	
Op	nergency perating ocedure	All	N/A	All		x		в	shutdown mode	Front. Syst. MSRT MHSI stop (1 train) Actuation Manual	Class 2	F1B	SAS	See Appendix A
					Heat removal		Transfer heat from the reactor coolant to the ultimate heat sink		Heat removal in shutdown	Front. Syst. MHSI MHSI injection on large miniflow	Class 2	F1B	SAS	
						x		B	mode by Residual Heat Removal system (RHRS)	Actuation Manual Front. Syst. MHSI LHSI switch to RHR mode (1 train)			343	
						x		В		Activ. & Elec Manual Front. Syst. RHRS	Class 2	F1B	SAS	
					Confinement	x	N/A	В		already effective due to automatic actu led, the operator can perform the conta			tomatic	
							x Shutdown and maintain core sub-criticality	в	Negative reactivity fast insertion	Reactor trip - auto Actuation PZR P HL P HL P Front. Syst. CRDM	Class 1	F1A	PS	
					Reactivity Control		x Prevention of uncontrolled			Turbine Trip Actuation RT checkback Front. Syst. Turbine admission valves	Class 1	F1A	PS	
							x positive reactivity insertion	В	RCS overcooling protection	Full load MFW isolation (4SG) Actuation RT checkback Front Syst Full load MFW	Class 1	F1A	PS	
							x			SG Pressure Control - Cooling Actuation Manual	Class 2	F1B	SAS	
							x Maintain sufficient Reactor Coolant System water	В	Water injection into the RCS	Front. Syst. MSRT MHSI injection - Auto Actuation SIS signal [PZR P] Front. Syst. MHSI	Class 1	F1A	PS	
							inventory for core cooling	в	Prevention of RCS drainage through auxiliary lines	Isolation of CVCS Low Pressure letdown line (RCS isolation SI sequence) Actuation SIS signal [PZR P] Front. Syst. CVCS letdown valve	Class 1	F1A	PS	
							x		Heat removal by Steam Generators - Emergency shutdown mode	SG Pressure Control - Cooling Actuation SG P Front. Syst. MSRT	Class 1	F1A	PS	
cm² v	A up to 20 with loss of partial	RRC-A	-	16.1.3.6	Heat removal		x			LHSI switch to RHR mode (1 train) Activ. & Elec Manual Front. Syst. RHRS	Class 2	F1B	SAS	N/A - diversity is applied to frequent initiating event above 10-3/r.y
	lown signal t power)						x			IRWST cooling Actuation SIS signal [PZR P]	Class 1	F1A	PS	
							Transfer heat from the reactor coolant to the ultimate heat sink		Heat removal in shutdown mode by Residual Heat Removal system (RHRS)	Front. Syst. RHRS Accumulators injection Actuation Passive Front. Syst. Accumulators	Class 1	F1A	PS	
							x			LHSI injection in CL Actuation SIS signal [PZR P] Front. Syst. LHSI	Class 2	F1B	PS	
							x			IRWST borated water storage, collect, filtration Actuation Passive Front. Syst. IRWST systems	Class 1	F1A	PS	
							x		Heat removal by Steam Generators - Emergency shutdown mode	EFW actuation (1 train) + SG Actuation SG L Front. Syst. EFWS injection lines & storages	Class 1	F1A	PS	
					Other		x Prevent the failure or limit th consequences of failure of a structure, system or component whose failure	в	Essential component protection	SG Pressure Control - Overpressure protection Actuation SG P Front. Syst. MSRT RCP stop - Auto	Class 1	F1A	PS	
							could cause the impairment of a safety function)T		Actuation DP over RCP + SIS signal Front. Syst. RCP Containment isolation stage 1 /	Class 1	F1A	PS	
					Confinement		Limit the release of radioactive material from the reactor containment	в	Containment building isolation	Actuation SIS signal [PZR P] Front. Syst. Containment isolation valves	Class 1	F1A	PS	



PAGE : 26 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

PRE-CONSTRUCTION SAFETY REPORT

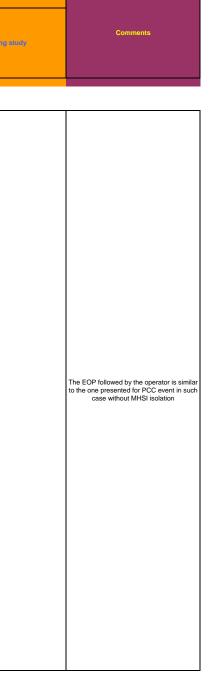
Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (9/29)

		Inpu	ut to clas	sification	1				SAFETY FUNCTION	N		MAIN	LINE					DIV	ERSE LINE		
		Referenc				Trop	nsient pl	haces	Plant Level Safety Function		Lower Level Safety Function		Safety Functional (Broups			Lower Level Safety Function	Safety Functional G	roups		
Fault descriptio		Referenc	.es		Main Safety Function	ITall	isient pi		Based on EPR process and international practice for		Combination of the Plant Level Safety Function and the			Safety	System	C&I platform	Combination of the Plant Level Salety Function and the		Safety	Syst	Supporting
, i	Category	Freq	luency	PCSR Ref.		Cont. state	Safe state	Final state	International practice for PWR		conditions of operations (normal, incident, accident)		ltem	class	Req.		conditions of operations (normal, incident, accident)	ltern		Koq.	
Decrease in	RCS water invento	ry																			•

					x	Shutdown and maintain core sub-criticality	В	Negative reactivity fast insertion	Reactor trip - auto Actuation PZR P HL P Front. Syst. CRDM	Class 1	F1A	PS	
				Reactivity Control	x	Prevention of uncontrolled	в		Turbine Trip Actuation RT checkback Front. Syst. Turbine admission valves	Class 1	F1A	PS	
					x	 positive reactivity insertion into the core 	в	RCS overcooling protection	Full load MFW isolation (4SG) Actuation RT checkback Front. Syst. Full load MFW isolation valves	Class 1	F1A	PS	
					x				SG Pressure Control - Cooling Actuation SIS signal [PZR P] Front. Syst. MSRT	Class 1	F1A	PS	
					x	Maintain sufficient Reactor	В	Water injection into the RCS	SG Pressure Control - Cooling Actuation Manual	Class 2	F1B	SAS	
					x	Coolant System water inventory for core cooling			Front. Syst. MSRT LHSI injection in CL Actuation SIS signal [PZR P] Front. Syst. LHSI	Class 1	F1A	PS	
					x		в	Prevention of RCS drainage through auxiliary lines	Isolation of CVCS letdown line (RCS isolation SI sequence) Actuation SIS signal [PZR P] Front. Syst. CVCS letdown valve	Class 1	F1A	PS	
LOCA up to 20					x			Heat removal by Steam Generators - Emergency shutdown mode	SG Pressure Control - Cooling Actuation SG P Front. Syst. MSRT	Class 1	F1A	PS	
cm ² without MHSI (at power)	RRC-A	-	16.1.3.7	Heat removal	x				LHSI switch to RHR mode (1 train) Activ. & Elec Manual Front. Syst. RHRS	Class 2	F1B	SAS	N/A - diversity is applied to frequent initiating event above 10-3/r.y
					x	-		Heat removal in shutdown	IRWST cooling Actuation SIS signal [PZR P] Front. Syst. RHRS	Class 1	F1A	PS	
					x	Transfer heat from the reactor coolant to the ultimate heat sink	В	mode by Residual Heat Removal system (RHRS)	Accumulators injection Actuation Passive Front. Syst. Accumulators LHSI injection in CL	Class 1	F1A	PS	
					x	_			Actuation SIS signal [PZR P] Front. Syst. LHSI IRWST borated water storage, collect. filtration	Class 2	F1B	PS	
					x	_		Heat removal by Steam	Actuation Passive Front. Syst. IRWST systems EFW actuation (1 train) + SG Actuation SG L	Class 1	F1A	PS	
					x	Prevent the failure or limit the		Generators - Emergency shutdown mode	Front. Syst. EFWS injection lines & storages SG Pressure Control - Overpressure protection	Class 1	F1A	PS	
				Other	x	component whose failure could cause the impairment of	в	Essential component protection	Actuation SG P Front. Syst. MSRT RCP stop - Auto	Class 1	F1A	PS	
						a safety function			Actuation bir over icon 4 signal Front. Syst. RCP Containment isolation stage 1 / Actuation SIS signal [PZR P]	Class 1	F1A	PS	
				Confinement	x	radioactive material from the reactor containment	В	Containment building isolation	Front. Syst. Containment isolation valves	Class 1	F1A	PS	L





CHAPTER 14: DESIGN BASIS ANALYSIS

SUB-CHAPTER : 14.7

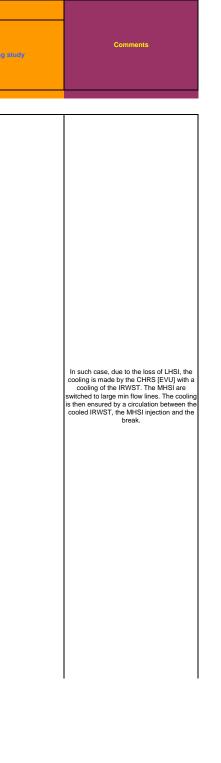
PAGE : 27 / 58

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (10/29)

		Input to cla	ssification					SAFETY FUNCTION	N		MAIN LINE				DVERSELINE	
	R	eferences			Tran	sient pha	ises P	Plant Level Safety Function		Lower Level Safety Function	Safety Functional C	Groups			Lower Level Balacy Functional Groups	
Fault description Decrease in RCS	Category	Frequency	PCSR Ref.	Main Safety Function	Cont. state	Safe state	1	Based on EPR process and international practice for PWR	Safety Cal	Combination of the Plant Level Safety Function and the conditions of operations (normal, incident, accident)	Item	Safety class	System Req.	C&I platform		ipporting (
															-	
							x ^s	Shutdown and maintain core sub-criticality	В	Negative reactivity fast insertion	Reactor trip - auto Actuation PZR P HL P HL P	Class 1	F1A	PS		
				Reactivity Control			x				Front. Syst. CRDM Turbine Trip Actuation RT checkback Front Surt Turbine admission	Class 1	F1A	PS		
							x	Prevention of uncontrolled positive reactivity insertion into the core	В	RCS overcooling protection	Front. Syst. valves Full load MFW isolation (4SG) Actuation RT checkback Actuation RT checkback Full load MEW	Class 1	F1A	PS		
							x				Front. Syst. Full load wirw isolation valves SG Pressure Control - Cooling	Class 2	F1B	SAS		
								Maintain sufficient Reactor Coolant System water	В	Water injection into the RCS	Actuation Manual Front. Syst. MSRT MHSI injection - Auto	Class 1	F1A	PS		
							x	inventory for core cooling	в	Prevention of RCS drainage	Actuation SIS signal [PZR P] Front. Syst. MHSI Isolation of CVCS letdown line (RCS isolation SI sequence) Actuation SIS signal [PZR P]		F1A	PS		
							^			through auxiliary lines Heat removal by Steam	Front. Syst. CVCS letdown valve		110			
							x			Generators - Emergency shutdown mode	Actuation SG P Front. Syst. MSRT	Class 1	F1A	PS		
LOCA up to 20 cm ² without LHSI (at power)	RRC-A	-	16.1.3.8	Heat removal			x				LHSI switch to RHR mode (1 train) Activ. & Elec Manual Front. Syst. RHRS	Class 2	F1B	SAS	N/A - diversity is applied to frequent initiating event above 10-3/r.y	
								ransfer heat from the reactor		Heat removal in shutdown	IRWST cooling Actuation SIS signal [PZR P] Front. Syst. RHRS	Class 1	F1A	PS		
							x	coolant to the ultimate heat sink	В	mode by Residual Heat Removal system (RHRS)	Accumulators injection Actuation Passive Front. Syst. Accumulators LHSI injection in CL	Class 1	F1A	PS		
							x				Actuation SIS signal [PZR P] Front. Syst. LHSI IRWST borated water storage, collect, filtration	Class 2	F1B	PS		
							x			Heat removal by Steam	Actuation Passive Front. Syst. IRWST systems EFW actuation (1 train) + SG Actuation SG L	Class 1	F1A	PS		
							x			Generators - Emergency shutdown mode	Front. Syst. EFWS injection lines & storages SG Pressure Control - Overpressure protection	Class 1	F1A	PS		
				Other			x	Prevent the failure or limit the consequences of failure of a structure, system or component whose failure	в	Essential component protection	Actuation SG P	Class 1	F1A	PS		
							0	ould cause the impairment of a safety function			Actuation DP over RCP + SIS signal Front. Syst. RCP Containment isolation stage 1/	Class 1	F1A	PS		
				Confinement			x r	Limit the release of radioactive material from the reactor containment	В	Containment building isolation	RCPB isolation Actuation SIS signal [PZR P] Front. Syst. Containment isolation valves	Class 1	F1A	PS		

UK EPR



CHAPTER 14: DESIGN BASIS ANALYSIS

SUB-CHAPTER : 14.7

PAGE : 28 / 58

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (11/29)

	Input to clas	ssificatior	n			SAFETY FUNCTIO	N		MAIN LINE					DIVER	SE LINE	
Fault description	eferences Frequency	PCSR Ref.	Main Safety Function	Transie Cont. S state s	ent phases Safe Final state state	Plant Level Safety Function Based on EPR process and international practice for PWR		Lower Level Safety Function Combination of the Plant Level Safety Function and the conditions of operations (normal, incident, accident)	Safety Function	System Req.	C&I platform	Lower Level Safety Function Contribution of the Plant Loop Safety Function and the Safety Function and operations (normal insolute, escability)	Safety Funct		ps Dafety Sy class Ro	Biggenting au

				Heat removal	x		Maintain sufficient Reactor Coolant System water inventory for core cooling	A	Water injection into the RCS	MHSI in Actuation Front, Syst.	njection - auto SIS signal [RCS L] SIS signal [ΔPsat] MHSI	Class 1 F	1A	PS	Water injection into the RCS		ection - auto Diversified RCS L MHSI	Class 2	F2	SAS	-	
Uncontrolled RCS level drop (states C3, D)	PCC2 f>10°/(r.y)	1.10 ⁻²	14.3.16	Heat removal	x		Maintain sufficient Reactor Coolant System water inventory for core cooling	A	Prevention of RCS drainage through auxiliary lines	Isolation of C (RCS isolat Actuation	CVCS letdown line tion SI sequence)	Class 1 F	1A	PS	Prevention of RCS drainage	Isolation of CV (RCS isolation	/CS letdown line on SI sequence) Diversified RCS L	Class 2	F2	SAS		
								A	Water injection into the RCS		hjection - Auto SIS signal [ΔPsat] MHSI	Class 1 F	1A	PS		MHSI Actuation Front, Syst,	injection Manual MHSI	Class 2	F1B	SAS		
Small break (not greater than DN 50) including a break occurring	PCC3			Heat removal	x		Maintain sufficient Reactor Coolant System water inventory for core cooling	A	Prevention of RCS drainage through auxiliary lines	Isolation of 0 (RCS isolat Actuation	CVCS letdown line tion SI sequence)	Class 1 F	1A	PS	Prevention of RCS drainage through auxiliary lines	Isolation of CN	/CS letdown line Manual CVCS letdown valve	Class 2	F1B	SAS		
on the Extra Boration System injection line (state B)	10-4/(r.y) <f<10- 2/(r.y)</f<10- 	•	14.4.5	Other	x		Prevent the failure or limit the consequences of failure of a structure, system or component whose failure could cause the impairment of a safety function	A	Essential component protection	Actuation	stop - Auto DP over RCP + SIS signal RCP	Class 1 F	1A	PS	Essential component protection	RCP ste Activ. & Elec Front. Syst.	op - Manu Manual RCP	Class 2	F1B	SAS	-	No challenge of reactivity control function
				Confinement	x		Limit the release of radioactive material from the reactor containment	A	Containment building isolation		t isolation stage 1 / SIS signal [ΔPsat] Containment isolation valves	Class 1 F	1A	PS	Containment building isolation	Containm Actuation Front. Syst.	ent isolation Manual Containment isolation valves	Class 2	F1B	SAS	-	
Small break LOCA (not greater than DN 50) including a break in the EBS injection line (states C1, C2)	PCC-4 10-6/(r.y) <f<10- 4/(r.y)</f<10- 	-	14.5.7		N/A							is similar to the	SB LOC/	A in state	B, in terms of systems actuation. (One MHSI pump	b is sufficient to man	age the sec	quence.			
								A	Water injection into the RCS	MHSI in Actuation Front. Syst.	njection - Auto SIS signal [RCS L] SIS signal [ΔPsat] MHSI	Class 1 F	1A	PS								
Isolable Safety Injection System break (≤ DN 250) in residual heat	PCC-4 10-6/(r.y) <f<10- 4/(r.y)</f<10- 	-	14.5.14	Heat removal	x		Maintain sufficient Reactor Coolant System water inventory for core cooling	A	Prevention of RCS drainage through auxiliary lines	Isolation of C (RCS isolat Actuation	CVCS letdown line tion SI sequence)	Class 1 F	1A	PS		N/A - dive	ersity is applied to free	equent initia	ating event	above 10	-3/r.y	Only the main features of the mitigation are presented. The heat removal is ensured thanks ot the other RHRS trains. Reactivity control is not impaired.
removal mode (states C, D)					x			A	Heat removal from containment by Containment Heat Removal system (CHRS)	Actuation Front. Syst.	Manual CHRS	Class 2	F2	SAS								There is no specific EOP since the transient occur in shutdown state.
				Confinement	x		Limit the release of radioactive material from the reactor containment	A	Containment building isolation	Actuation	t isolation stage 1 / SIS signal [RCS L] SIS signal [ΔPsat] Containment isolation valves	Class 1 F	1A	PS								
Uncontrolled RCS level drop without SI signal from PS (in shutdown state)	RRC-A	-	16.1.3.9	Heat removal		x	Maintain sufficient Reactor Coolant System water inventory for core cooling	В	Prevention of RCS drainage through auxiliary lines	Actuation	CVCS letdown line RCS L CVCS letdown valve	Class 3 I	F2	PS		N/A - dive	ersity is applied to free	equent initia	ating event	above 10		Only the main features of the mitigation are presented. The heat removal is ensured thanks ot the RHRS trains. Reactivity control is not impaired. There is no specific EOP since the transient occur in shutdown state.

UK EPR



PAGE : 29 / 58

PRE-CONSTRUCTION SAFETY REPORT

UK EPR

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

Safety Functional Groups Supporting study Safety Function and the conditions of operations Safety class Syst Req. Safety class ional prac PWR System Req. Item Cont. Safe Fina PCSR Category Frequent Emergency boron injection into the core - diversified Reactor trip PZR P Manual ATWS signal (N-3 rod drop) High concentrated and high pressure boron injection wn and maintain sub-criticality PS А F1A PS F2 ATWS cover egative reactivity fast in Actuation lass 1 Actuation Front. Syst. CRDM Front. Syst. EBS Reactor trip - auto Reactivity Control HL P hutdown and maintain co Negative reactivity fast insertion Actuation F2 SAS А sub-criticality Front. Syst. CRDM MSIV closure ation SG P Actuation RT checkback Front. Syst. Turbine admission valves F1A PS Actuation F1A PS lass 1 Excessive increase in steam flow stu Prevention of uncontrol positive reactivity insert into the core Front. Syst. MSIV А RCS ove RCS Full load MFW isolation (4SG SAS order in case of ATWS following PS failure RT checkback Full load MFW lass 1 F1A PS F2 SAS Full load MFW Front. Syst. Front, Syst. SG Pressure Control - Cooling -Covered by LOCA (BREAK SIZE UP TO 20 CM2) WITH FAILURE OF THE PARTIAL COOL-DOWN SIGNAL (STATE A) - PCSR Sub-chapter 16.1.3.3.6 Manu Actuation SIS signal [PZR P] lass 1 F1A PS Actuation Manual F1B SAS MSRT MSRT Front. Syst. Front. Syst. А Water injection into the RCS Water injection into the RCS PCC-3 10-4/(r.y)<f<10-2/(r.y) Covered by LOCA (BREAK SIZE UP TO 20 CM2) WITHOUT MHSI (STATE A) - PCSR Sub-chapter 16.1.3.3.7 LHSI in cold leg Maintain sufficient Reactor Coolant System water inventory for core cooling MHSI injection - Auto Generator tub upture (1 tube 9.8.10⁻⁴ 14.4.6 F1B F1A PS lass 1 Actuation SIS signal [PZR P] Front. Syst. MHSI Actuation Manual Front. Syst. LHSI Steam solation of CVCS letdown line (RCS isolation SI sequence) Isolation of CVCS letdown line Senerator tube upture (2 tubes n 1 SG) (State Prevention of RCS drainage through auxiliary lines Prevention of RCS drainage through auxiliary lines PCC-4 0-6/(r.y)<f<10-4/(r.y) А F1A F1B SAS lass 1 PS Actuation SIS signal [PZR P] Actuation Manual 14.5.10 2.10⁻⁴ Front. Syst. CVCS letdown valve Front. Syst. CVCS letdown valve SG Pressure Control - Cooling SG Pressure Control - Cooling SG Pressure Comment Actuation SG P Front. Syst. MSRT Trive actuation (1 train) + SG F1A PS F1B SAS Actuation Manual Front. Syst. MSRT Heat removal by Steam Generators - Emergency shutdown mode Heat removal by Low He Emergency Core Coolin System (ECCS) insfer heat from the colant to the ultima sink te heat Α EFW actuation (1 train) Blowdown Isolation Actuation SG L Front. Syst. EFWS injection lines & storages F1B SAS F1A lass 1 PS Actuation Manual Front. Syst. EFWS ent the failure or limit event the failure or limit the insequences of failure of a structure, system or component whose failure SG safety valves opening Secondary overpressure studies of Sub-chapter 3.4.1.5 illustrate Other x Δ F1A PS F1A lass 1 Actuation SG P Front. Syst. MSRT Actuation Passive Front. Syst. MSSV Id cause the impairment Steam line isolation (1SG) Steam line is tion (1SG) F1B F1A PS SAS Class 1 Actuation SG L + PCD finished Actuation Manual Front. Syst. MSIV Front. Syst. MSIV Isolation of CVCS charging line Isolation of CVCS charging line imitation of radioactive release outside containment from radioactive Steam Generator F1A PS F1B SAS Class 1 Limit the release of waste and airborne radioactive material Actuation SG L + PCD finished Manual Actuation lease outside containme from radioactive Steam А Front. Syst. CVCS Front. Syst. CVCS MSRT setp MSRT setpoint increase - Auto oint increase - Man F1A F1B SAS lass 1 PS Actuation SG L + PCD finished Actuation Manual Front. Syst. MSRT Front. Syst. MSRT Emergency boron injection into the core - Manual utdown and maintain co sub-criticality Compensation for shutdow Reactivity Control F1B в lass 2 SAS moderator effect Actuation Manual Front. Syst. EBS Heat removal by Steam Generators - Emergency shutdown mode SG Pressure Control - Cooling F1B в SAS lass 2 Actuation Manual Front. Syst. MSRT MHSI stop (1 train) x F1B SAS Class 2 Actuation SIS signal [PZR P] Front. Syst. MHSI insfer heat from the react colant to the ultimate hea sink Heat removal in shutdown mode by Residual Heat Removal system (RHRS) SG Pressure Control - Cooling F1B SAS в lass 2 Actuation Manual Front. Syst. MSRTa Emergency Operating Procedure AII N/A HSI switch to RHR mode (1 train See Appendix A All в F1B SAS lass 2 ctiv. & Elec Manual ront. Syst. RHRS Steam line isolation (1SG) F1B SAS Actuation Manual Front. Syst. MSIV iss 2 nitation of radioactive rele Limit the release of waste and airborne radioactive material в outside containment from adioactive Steam Generato F1B SAS lass 2 Actuation Manual Front. Syst. MSRT revent the failure or limit the Actuation Manual EFWS injection lines Prevent the failure or limit the consequences of failure of a structure, system or component whose failure ould cause the impairment of a safety function F1B lass 2 SAS Front. Syst. & storages Other sential component prote Actuation Manual Front. Syst. EFWS injection lines & storages F1B lass 2 SAS

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (12/29)

Comments
The occurrence of SG level as RT depends
on the level of power of the plant is operated. Manual RT of main line is actuated by
operator on KRT VVP detecors which are class 1 (F1A).
The operator may perform a fast cooldown with the 3 unaffected SGs to cool down the plant. This action will be performed locally
after 1 hour. The combination of SGTR + failure of all MSRT leads to a transient enough
unfrequent to limit the requirements in terms of diversity.
In case of failure of MSRTa setpoint increase and SGa isolation, the operator can also isolate the unaffected SGs by
closing the other MSIV in case of single failure of the MSIV of SGa
MHSI stop (1 train) is indicated combined with RHRS actuation since it is one of the
conditions to connect RHRS in such case. The same reasoning is applied for the opening of MSRT of the SGa to perform the
depressurization of both RCS and SGa in the end of the transient. LHSI injection in HL is only used in case of
LB LOCA.

UK EPR		PRE-CONSTRUCTION SAFETY REPORT	SUB-CHA	PTER : 14.
	UK EPR			: 30 /
Document ID.N UKEPR-0002-149 Is:		CHALLER 14. DEGION BAGIG ANALTOIS		

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (13/29)

		Input to cla	assificatio	n					ON		MAIN	LINE						DIV	ERSE LINE			
Fault description	R	eferences		Main Safety Function	Trar	nsient p	ohases	Plant Level Safety Function Based on EPR process and	Safety Cat.	Lower Level Safety Function Combination of the Plant Level Safety Function and the		Safety Functional				Lower Level Safety Function Combination of the Plant Leve Safety Function and the		Safety Functional G				Supporting study
Increase in Heat	Category	Frequency	PCSR Ref.	Function	Cont. state	Safe state	Final state	international practice for PWR		conditions of operations (normal, incident, accident)		ltem	Safety class	System Req.		conditions of operations (normal, incident, accident)		ltem	Safety class	Syst Req.		
Feedwater malfunction - T _{mfws} decrease	PCC-2 f>10-2/(r.y)	> 1.10 ⁻²	14.3.1				N/A							Tra	ansient not :	studied in the PCSR - part of Site	Licensing					
Feedwater malfunction - Q _{mfws} increase	PCC-2 f>10-2/(r.y)	> 1.10 ⁻²	14.3.2				N/A							Tra	ansient not :	studied in the PCSR - part of Site	Licensing					
											Reac	tor trip - auto						boron injection into re - diversified				
					x			Shutdown and maintain core sub-criticality	А	Negative reactivity fast insertion	Actuation	DNBR or HCPL	Class 1	F1A	PS	High concentrated and high pressure boron injection	Actuation	ATWS signal (N-3 rod drop)	Class 2	F2	PS	PCSR Sub-chapter 16.1.3.3. Excessive increase in steam f drop failure
											Front. Syst.	CRDM					Front. Syst.	EBS				
																	Read	tor trip - auto				
				Reactivity Control	x			Shutdown and maintain core sub-criticality	A							Negative reactivity fast insertion	Actuation	SG L	Class 2	F2	SAS	
Excessive	PCC-2		14.3.3								Tu	rbine Trip					Front. Syst.	CRDM SIV closure				
increase in secondary steam flow	f>10-2/(r.y)	7.5.10 ⁻²	14.0.0		x						Actuation Front. Syst.	RT checkback Turbine admission valves	Class 1	F1A	PS		Actuation Front. Syst.	SG P MSIV	Class 1	F1A	PS	Excessive increase in steam f
					x			Prevention of uncontrolled positive reactivity insertion	A	RCS overcooling protection	Full load M Actuation Front. Syst.	FW isolation (4SG) RT checkback Full load MFW isolation valves	Class 1	F1A	PS	RCS overcooling protection	Full load M Actuation Front. Syst.	FW isolation (4SG) RT checkback Full load MFW isolation valves	Class 2	F2	SAS	SAS order in case of ATWS fol failure
Small steam system piping	PCC-3 10-4/(r.y) <f<10-< td=""><td>2.10⁻³</td><td></td><td></td><td>x</td><td></td><td></td><td>into the core</td><td></td><td></td><td>Low load M Actuation Front. Syst.</td><td>FW isolation (1SG) SG P Low load MFW isolation valves</td><td>Class 1</td><td>F1A</td><td>PS</td><td></td><td>Low load M Actuation Front. Syst.</td><td>IFW isolation (1SG) Manual Low load isolation valves</td><td>Class 2</td><td>F2</td><td>SAS</td><td></td></f<10-<>	2.10 ⁻³			x			into the core			Low load M Actuation Front. Syst.	FW isolation (1SG) SG P Low load MFW isolation valves	Class 1	F1A	PS		Low load M Actuation Front. Syst.	IFW isolation (1SG) Manual Low load isolation valves	Class 2	F2	SAS	
failure to SG	2/(r.y)	2.10	14.4.1		x						Activ. & Elec	e isolation (1SG) SG P	Class 1	F1A	PS		Activ. & Elec	he isolation (1SG) Manual	Class 2	F1B	SAS	-
					x						Front. Syst. SG Pressur Actuation Front. Syst.	e Control - Cooling SG P	Class 1	F1A	PS		Front. Syst. Opening Actuation Front. Syst.	MSIV of severe accident Manual PDS	Class 2	F2	SAS	
				Heat removal	x			Transfer heat from the reactor coolant to the ultimate heat sink	A	Heat removal by Steam Generators - Emergency shutdown mode		tion (1 train) + SG SG L EFWS injection lines & storages	Class 1	F1A	PS	Heat removal by Low Head Emergency Core Cooling System (ECCS)	Actuation Front. Syst.	IS] in cold leg Manual MHSI + LHSI	Class 2	F1B	SAS	Sequences of primary bleed detailed in case of Total Loss Of RRC-A
					x							d biologoo					RCP Activ. & Elec Front. Syst.		Class 2	F1B	SAS	
				Other	x			consequences of failure of a structure, system or component whose failure	А	Essential component protection	Overpre: Actuation	ssure Control - ssure protection SG P	Class 1	F1A	PS	Essential component protection	SG safet	y valves opening Passive	Class 1	F1A	-	Secondary overpressure studi chapter 3.4.1.5 illustra
				Confinement	x			Maintain integrity of the Reactor Coolant Pressure Boundary	A	RCS overpressure protection	Front. Syst. Hot overpu Actuation Front. Syst.	MSRT essure protection Passive PSV	Class 1	F1A	-	RCS overpressure protection			Class 1	F1A	-	Primary overpressure studies chapter 3.4.1.5 illustra

udy	Comments
.3.3.1 - ATWS am flow by rod	
eam flow study	
/S following PS	
leed and feed ss Of FeedWater	
studies of Sub- ustrate	
udies of Sub- ustrate	

PAGE : 31 / 58

PRE-CONSTRUCTION SAFETY REPORT

UK EPR

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (14/29)

		Input to cla	ssificatio	on				SAFETY FUNCTION	N		MAIN	LINE						DIV	ERSE LINI			
Fault	R	eferences		Main Safet		ansient	phases	Plant Level Safety Function Based on EPR process and	Safety Cat	Lower Level Safety Function Combination of the Plant Level		Safety Functional (Lower Level Safety Function		Safety Functional G			-	Supporting s
description	Category	Frequency	PCSR Ref.	Function	Con stat	t. Safe e state	e Final e state	international practice for PWR		Safety Function and the conditions of operations (normal, incident, accident)		ltem	Safety class	System Req.		Safely Function and the conditions of operations (normal, incident, actident)		ltem	Safety class	Syst Req.		
	Removal								1								T					
											Reac	tor trip - auto						boron injection into ore - diversified				
					x				A	Negative reactivity fast insertion	Actuation	DNBR or HCPL	Class 1	F1A	PS	High concentrated and high pressure boron injection	Actuation	ATWS signal (N-3 rod drop)	Class 2	F2	PS	PCSR Sub-chapter 16.1 Excessive increase in ste drop failure
								Shutdown and maintain core sub-criticality			Front. Syst.	CRDM					Front. Syst.	EBS				
										High concentrated boron		boron injection into core - Auto				High concentrated and high		boron injection into core - manu				
					x				A	injection	Activ. & Elec	SG P	Class 1	F1A	PS	pressure boron injection	Actuation	Manual	Class 2	F2	PS	
				Reactivity Control							Front. Syst.	EBS					Front. Syst.	EBS				
					x						Actuation Front. Syst.	rbine Trip RT checkback Turbine admission valves	Class 1	F1A	PS		Actuation Front. Syst.		Class 1	F1A	PS	Excessive increase in ste
Inadvertent					x						Full load M Actuation Front. Syst.	FW isolation (4SG) RT checkback Full load MFW isolation valves	Class 1	F1A	PS		Full load M Actuation Front. Syst.	Full load MEW	Class 2	F2	SAS	SAS order in case of ATV failure
opening of a SG relief train or of a Safety valve	PCC-3 10-4/(r.y) <f<10- 2/(r.y)</f<10- 	> 10 ⁻³	14.4.4		x			Prevention of uncontrolled positive reactivity insertion into the core	A	RCS overcooling protection	Low load M Actuation Front. Syst.	FW isolation (1SG) SG P Low load MFW isolation valves	Class 1	F1A	PS	RCS overcooling protection	Low load M Actuation Front. Syst.	MFW isolation (1SG) Manual	Class 2	F2	SAS	
(state A)					x						Steam lin Activ. & Elec Front. Syst.	e isolation (1SG) SG P	Class 1	F1A	PS		Steam lin Activ. & Elec Front. Syst.	ne isolation (1SG) Manual	Class 2	F1B	SAS	-
					x			-			MSRT isola Activ. & Elec Front. Syst.	tion (1 SG isolation SG P MSRT	Class 1	F1A	PS		MSRT isola Activ. & Elec Front. Syst.	ation (1 SG isolation Manual MSRT	Class 2	F1B	SAS	-
					x			Maintain sufficient Reactor Coolant System water	А	Water injection into the RCS	Au	Control - Cooling - to (MSRT) SIS signal [PZR P] MSRT	Class 1	F1A	PS	Water injection into the RCS	Actuation Front. Syst.	Manu Manual MSRT	Class 2	F1B	SAS	-
					x			inventory for core cooling			MHSI i Actuation Front. Syst.	njection - Auto SIS signal [PZR P] MHSI	Class 1	F1A	PS		Actuation Front. Syst.	LHSI	Class 2	F1B	SAS	-
				Heat remov	al x						SG Pressur Actuation Front. Syst.	e Control - Cooling SG P MSRT	Class 1	F1A	PS			of severe accident scharge line Manual PDS	Class 2	F2	SAS	
					x			Transfer heat from the reactor coolant to the ultimate heat sink	A	Heat removal by Steam Generators - Emergency shutdown mode		ttion (1 train) + SG SG L EFWS injection lines & storages	Class 1	F1A	PS	Heat removal by Low Head Emergency Core Cooling System (ECCS)	SIS [R Actuation Front. Syst.		Class 2	F1B	SAS	Sequences of primary b detailed in case of Total Lo RRC-A
					x			1				2.2.3.0900					RCP Activ. & Elec Front. Syst.		Class 2	F1B	SAS	1
				Other	x			consequences of failure of a structure, system or component whose failure	А	Essential component protection		ssure Control - ssure protection SG P MSRT	Class 1	F1A	PS	Essential component protection		ty valves opening Passive	Class 1	F1A	-	Secondary overpressure : chapter 3.4.1.5 ill

) study	Comments
6.1.3.3.1 - ATWS steam flow by rod lure	
steam flow study	
TWS following PS	
y bleed and feed Loss Of FeedWater A	
re studies of Sub- 5 illustrate	

PAGE : 32 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

PRE-CONSTRUCTION SAFETY REPORT

UK EPR

Document ID.No. UKEPR-0002-149 Issue 03

						ę	SUE	B-CHAPTER 1	4.7 - T	ABLE 1: FAUL		PROTEC	TION	SCH	EDUL	_E TABLE: FAULTS AT FULL POWER (15/29)
		Input to cl	assificatio	n				SAFETY FUNCTION	N		MAIN	LINE				BIVERSE LINE
Fault description	R	eferences Frequency	PCSR Ref.	Main Safety Function	Tra Cont	nsient p t. Safe state	hases Final state	Plant Level Safety Function Based on EPR process and international practice for PWR	Safety Cat.	Lower Level Safety Function Combination of the Plant Level Safety Function and the conditions of operations (normal, incident, accident)		Safety Functional G	Safety class	System Req.		Lemmer Levels Salety Fination Contributing Control Control Salety Functional Control Salety Function and Applications (normal Functions and Applications (normal Functions and Applications (normal Functions)
Increase in He	at Removal				×				A	Negative reactivity fast insertior	Actuation	ctor trip - auto dP/dt PZR P, SG P, Cont P, DNBR	Class 1	F1A	PS	
					x			Shutdown and maintain core sub-criticality	A	High concentrated boron injection	the Activ. & Elec	boron injection into core - Auto	Class 1	F1A	PS	
				Reactivity Control	x						Actuation Front. Syst.	Urbine Trip RT checkback Turbine admission valves	Class 1	F1A	PS	
					x			Prevention of uncontrolled positive reactivity insertion into the core	A	RCS overcooling protection	Actuation Front. Syst. EFW i	Full load MFW isolation valves solation (1 SG)	Class 1	F1A	PS	
					x x			_			Activ. & Elec	ne isolation (1SG) dP/dt, SG P	Class 1 Class 1	F1A F1A	PS PS	-
					x						Activ. & Elec	MSIV re Control - Cooling SG P	Class 1	F1A	PS	
Steam syster line break	10-6/(r.y) <f<10-< td=""><td>_</td><td>14.5.2</td><td></td><td>x</td><td></td><td></td><td>Transfer heat from the reacto coolant to the ultimate heat sink</td><td>r A</td><td>Heat removal by Steam Generators - Emergency shutdown mode</td><td>Front. Syst. EFW actu Blow Activ. & Elec Front. Syst.</td><td>ation (1 train) + SG down Isolation : SG L EFWS injection lines</td><td>Class 1</td><td>F1A</td><td>PS</td><td>N/A - diversity is applied to frequent initiating event above 10-3/r.y</td></f<10-<>	_	14.5.2		x			Transfer heat from the reacto coolant to the ultimate heat sink	r A	Heat removal by Steam Generators - Emergency shutdown mode	Front. Syst. EFW actu Blow Activ. & Elec Front. Syst.	ation (1 train) + SG down Isolation : SG L EFWS injection lines	Class 1	F1A	PS	N/A - diversity is applied to frequent initiating event above 10-3/r.y
(states A and	B) 4/(r.y)			Heat removal							SG Pressur	& storages re Control - Cooling - Auto SG P	Class 1	F1A	PS	
					x			Maintain sufficient reactor coolant system water inventory for core cooling	A	Water injection into the RCS	Front. Syst. MHSI Activ. & Elec Front. Syst.	injection - Auto	Class 1	F1A	PS	
								Prevent the failure or limit the	А	Prevention of RCS drainage through auxiliary lines		SIS signal	Class 1	F1A	PS	
				Other	x			consequences of failure of a structure, system or component whose failure could cause the impairment o a safety function	A	Essential component protection	Overnre	SG P MSRT	Class 1	F1A	PS	
								Limit the release of			Containme Actuation	ent isolation stage 1	Class 1	F1A	PS	
				Confinement	x			radioactive material from the reactor containment	A	Containment building isolation	Containme	isolation valves isolation stage 2 SIS signal [PZR P] Containment isolation valves	Class 1	F1A	PS	
Inadvertent opening of a S relief train or Safety valve (state B)	G PCC-4 10-6/(r.y) <f<10- 4/(r.y)</f<10- 	-	14.5.4					N/A	1		1	isolation valves	1	L		Transient covered by Steam piping break
						x			В	Compensation for shutdown moderator effect	Emergency the Actuation Front. Syst.	boron injection into core - Manual Manual EBS	Class 2	F1B	SAS	
				Reactivity Control		x		Shutdown and maintain core sub-criticality	в	RCS overcooling protection	Low load M Actuation Front. Syst. Steam lin	MFW isolation (4SG) Manual Full load MFW isolation valves ne isolation (1SG)	Class 2	F1B	SAS	
Emergency Operating Procedure	All	N/A	All			x			в	Heat removal by Steam Generators - Emergency shutdown mode	Activ. & Elec Front. Syst. SG Pressu Actuation		Class 2 Class 2	F1B F1B	SAS SAS	See Appendix A N/A
				Heat removal				Transfer heat from the reacto coolant to the ultimate heat sink	rв	-	Front. Syst.	MSRT essurisation by PZR Manual	Class 2	F1B	SAS	
						x			в	Heat removal in shutdown mode by Residual Heat Removal system (RHRS)	RHR connec	ction and start-up (no SI signal) Manual	Class 2	F1B	SAS	

g study	Comments
A	

PAGE : 33 / 58

PRE-CONSTRUCTION SAFETY REPORT

UK EPR

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (16/29)

Input to classification								SAFETY FUNCTION MAIN LINE									VID	ERSE LINE			
	References			Tra	Transient ph		Plant Level Safety Function		Lower Level Safety Function		roups			Lower Level Safety Functio	Safety Functional G	oups					
Fault description				Main Safety Function		nsient phase		Based on EPR process and international practice for	Safety Cat	Combination of the Plant Level Safety Function and the conditions of operations		ltem		System		Combination of the Plant Level Safety Function and the	ltem		Syst	Supporting study	Comments
	Category	Frequency	PCSR Ref.		Cont state		Final state	PWR		(normal, incident, accident)			class	Req.		conditions of operations (normal, incident, accident)		class f	Req.		
Decrease in Heat	PCC-2 f>10-2/(r.y)										Reactor trip - auto						Emergency boron injection into the core - diversified				
					x	x	Shutdown and maintain core sub-criticality	e A	Negative reactivity fast insertion	Actuation PZR P		Class 1 F1A PS		PS	High concentrated and high	Actuation ATWS signal (N-3 rod drop)	Class 2	F2	PCSR Sub-chapter 16.1.3.3.1 - ATWS LOFW by rod drop failure covers the ATWS	ATWS are not postulated for PCC-3 and PCC-4 events	
										Front. Syst.					pressure boron injection	Front. Syst. EBS			LOCV	FOC-4 events	
				Reactivity Control							FIDIL Syst.	CRDM					Reactor trip - auto				
					x			Shutdown and maintain core sub-criticality	A						Negative reactivity fast insertion	Actuation HL P	Class 2	F2 5	AS		
Turbine Trip Loss of condenser vacuum											Tur	bine Trip					Front. Syst. CRDM MSIV closure				
					×			Prevention of uncontrolled positive reactivity insertion into the core			Actuation Front. Syst.	RT checkback Turbine admission valves	Class 1	F1A	PS	ŀ	Actuation SG P Front. Syst. MSIV	Class 1	F1A	S Excessive increase in steam flow study	TT initiating event
		2.5.10 ⁻¹ 1.5.10 ⁻¹			x						Actuation	RT checkback	Class 1	F1A	PS		Full load MFW isolation (4SG) Actuation RT checkback SG L Full load MFW Full load MFW	Class 2	F2 S	AS SAS order in case of ATWS following PS failure	
			14.3.4								Front. Syst. Steam line	isolation (1SG)				RCS overcooling protection	Front. Syst. isolation valves Steam line isolation (1SG)				Only in case of loss of condenser (1) due to the single failure on MSRIV and small
					x						Activ. & Elec Front. Syst.	MSIV	Class 1	Class 1 F1A PS	PS		Activ. & Elec Manual Front, Syst. MSIV	Class 2	F1B S	45 -	feedwater system piping (3) due to the break.
					x								Class 1	F1A	PS		MSRT isolation (1 SG isolation valve closure) Activ. & Elec Manual Front. Syst. MSRT	Class 2	F1B \$	4 S -	Only in case of loss of condenser (1), due to the single failure on MSRIV
					x	x	Transfer heat from the reactor coolant to the ultimate heat A		Heat removal by Steam Generators - Emergency		Control - Cooling	Class 1	F1A	PS		Opening of severe accident discharge line Actuation Manual	Class 2	F2 S	AS		
				Heat removal x				A		Front. Syst. EFW actuat Actuation	EFW actuation (1 train) + SG		Class 1 F1A PS	PS	Heat removal by Low Head Emergency Core Cooling	Front. Syst. PDS SIS [RIS] in cold leg Actuation Manual	Class 2 F1B	F1B S	Sequences of primary bleed and feed detailed in case of Total Loss Of FeedWater		
					×			sink		shutdown mode	Front. Syst.					System (ECCS)	Front. Syst. MHSI + LHSI RCP stop - Manu Activ. & Elec Manual	Class 2 F1B	F1B S	RRC-A	
				Other	~			Prevent the failure or limit the consequences of failure of a	re of a or A illure A ment of	Essential component protection		SG Pressure Control - Overpressure protection					Front. Syst. RCP SG safety valves opening				
					x			structure, system or component whose failure could cause the impairment of a safety function			Actuation Front. Syst.	SG P MSRT	Class 1	F1A	PS	Essential component protection	Actuation Passive Front. Syst. MSSV	Class I F	F1A	Secondary overpressure studies of Sub- chapter 3.4.1.5 illustrate	
				Confinement	x			Maintain integrity of the Reactor Coolant Pressure Boundary	А	RCS overpressure protection	Hot overpre Actuation Front. Syst.	Passive Passive PSV	Class 1	F1A	-	RCS overpressure protection	Hot overpressure protection Activ. & Elec Front. Syst. PSV	Class 1	F1A	Primary overpressure studies of Sub- chapter 3.4.1.5 illustrate	
	PCC-2 f>10-2/(r.y)	6.25.10 ⁻³										or trip - auto					Emergency boron injection into the core - diversified				
					x	Shutdown and maintain core sub-criticality	A	Negative reactivity fast insertion	Actuation	SG L PZR P	Class 1	F1A	PS	High concentrated and high pressure boron injection	Actuation ATWS signal (N-3 rod drop)	Class 2	F2 P	PCSR Sub-chapter 16.1.3.3.1 - ATWS LOMFW	A partial trip may occur before actuation of the RT on loss of normal feedwater. See Total Loss of FeedWater sequence below		
				Reactivity Control							Front. Syst.	CRDM					Front. Syst. EBS				
					x			Prevention of uncontrolled positive reactivity insertion	A	RCS overcooling protection		bine Trip RT checkback	Class 1	F1A	PS	RCS overcooling protection	MSIV closure Actuation SG P	Class 1	F1A	S Excessive increase in steam flow study	
								Transfer heat from the reactor coolant to the ultimate heat sink		Heat removal by Steam Generators - Emergency shutdown mode	Front. Syst.	Turbine admission valves					Front. Syst. MSIV Opening of severe accident				
Loss of normal feedwater flow			14.3.7	Heat removal	x						Actuation Front. Syst.	SG P MSRT	Class 1	lass 1 F1A PS		Heat removal by Low Head Emergency Core Cooling System (ECCS)	discharge line Actuation Manual Front. Syst. PDS	Class 2 F2 Class 2 F1B	F2 S	Sequences of primary bleed and feed detailed in case of Total Loss Of FeedWater RRC-A	
					x						EFW actuation (1 train) + SG Actuation SG L Front. Syst. EFWS injection lin & storages		S Class 1	F1A	PS		SIS [RIS] in cold leg Actuation Manual Front. Syst. MHSI + LHSI		F1B S		
					x							∝ storages					RCP stop - Manu Activ. & Elec Manual Front. Syst. RCP	Class 2	F1B S	AS	
				Other	x			Prevent the failure or limit the consequences of failure of a structure, system or		Essential component protection		sure Control - sure protection	Class 1	F1A	PS	Essential component protection	SG safety valves opening	Class 1 F1A	F1A	Secondary overpressure studies of Sub-	
								component whose failure could cause the impairment of a safety function Maintain integrity of the			Actuation Front. Syst. Hot overpre	MSRT				Losential component protection	Actuation Passive Front. Syst. MSSV			chapter 3.4.1.5 illustrate	
				Confinement	x			Reactor Coolant Pressure Boundary	A	RCS overpressure protection	Actuation Front. Syst.	Passive	Class 1	F1A	-	RCS overpressure protection	Hot overpressure protection Activ. & Elec Passive Front. Syst. PSV	Class 1	F1A	Primary overpressure studies of Sub- chapter 3.4.1.5 illustrate	

PAGE : 34 / 58

PRE-CONSTRUCTION SAFETY REPORT

UK EPR

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (17/29)

		Input to cla	assificatio	n			SAFETY FUNCTIO	N		MAIN I	LINE						DIVERSE LIN				
									Lower Level Safety Function		Safety Functional	Groups			Lower Level Safety Function		Safety Functional Groups				
Fault description		eferences	PCSR	Main Safety Function	Transient p	ohases Final	Plant Level Safety Function Based on EPR process and international practice for PWR	Safety Cat.	Combination of the Plant Level Safety Function and the conditions of operations		ltem	Safety class	System Req.		- Combination of the Plant Level Safety Function and the conditions of operations		Item Safety class	Syst Req.		Supporting study	Comments
Increase in Heat	Category	Frequency	Ref.		state state	state			(normal, incident, accident)						(normal, incident, accident)						
morease in ricat	Keliloval																				
					x		Shutdown and maintain core sub-criticality	A	Negative reactivity fast insertion	Reactor Actuation Front. Syst.	or trip - auto HCPL / DNBR SG P CRDM	Class 1	F1A	PS	High concentrated and high pressure boron injection		boron injection into re - diversified ATWS signal (N-3 rod drop) EBS	F2	PS	PCSR Sub-chapter 16.1.3.3.1 - ATWS LOFW	ATWS are not postulated for PCC-3 and PCC-4 events
					x		Shutdown and maintain core sub-criticality	A			<u>onom</u>				Negative reactivity fast insertion		tor trip - auto high neutron flux HL P CRDM	F2	SAS		
				Reactivity Control	x					Tur Actuation Front. Syst.	Turbine admission	Class 1	F1A	PS			SG P Class 1	F1A	PS	Excessive increase in steam flow study	
					x		Prevention of uncontrolled positive reactivity insertion into the core	A	RCS overcooling protection	-	valves FW isolation (4SG) RT checkback Full load MFW isolation valves	Class 1	F1A	PS	RCS overcooling protection	-	FW isolation (4SG) RT checkback Full load MFW isolation valves	F2	SAS	SAS order in case of ATWS following PS failure	
Small feedwater	PCC-3				x					Steam line Activ. & Elec Front. Syst.	sisolation (1SG) SG P MSIV	Class 1	F1A	PS		Steam lin Activ. & Elec Front. Syst.	e isolation (1SG) Manual Class 2	F1B	SAS	-	
system piping failure	10-4/(r.y) <f<10- 2/(r.y)</f<10- 	2.10 ⁻³	14.4.1		x						e Control - Cooling SG P	Class 1	F1A	PS		Opening o	charge line Manual	F2	SAS		
				Heat removal	x		Transfer heat from the reactor coolant to the ultimate heat sink	A	Heat removal by Steam Generators - Emergency shutdown mode		tion (1 train) + SG SG L EFWS injection lines & storages	Class 1	F1A	PS	Heat removal by Low Head Emergency Core Cooling System (ECCS)		IS] in cold leg Manual MHSI + LHSI	F1B	SAS	Sequences of primary bleed and feed detailed in case of Total Loss Of FeedWater RRC-A	
					x											RCP Activ. & Elec Front. Syst.	stop - Manu Manual RCP	F1B	SAS		
				Other	x		Prevent the failure or limit the consequences of failure of a structure, system or component whose failure could cause the impairment of a safety function	A	Essential component protection	Overpres Actuation	sure Control - sure protection SG P MSRT	Class 1	F1A	PS	Essential component protection	SG safety Actuation	y valves opening Passive	F1A	-	Secondary overpressure studies of Sub- chapter 3.4.1.5 illustrate	
				Confinement	x		Maintain integrity of the Reactor Coolant Pressure Boundary	А	RCS overpressure protection	Front. Syst. Hot overpre Actuation Front. Syst.	essure protection	Class 1	F1A	-	RCS overpressure protection	Front. Syst. Hot overpr Activ. & Elec Front. Syst.	Passive Class 1	F1A	-	Primary overpressure studies of Sub- chapter 3.4.1.5 illustrate	The overpressure protection is ensured thnaks to the 3 PSVs. It can be demonstrated that no CCF will impair the
					x		Shutdown and maintain core sub-criticality	A	Negative reactivity fast insertion		or trip - auto PZR P SG P CRDM	Class 1	F1A	PS	High concentrated and high pressure boron injection	Emergency	boron injection into re - diversified ATWS signal (N-3 rod drop)	F2	PS	PCSR Sub-chapter 16.1.3.3.1 - ATWS LOFW	
				Reactivity Control	x		Prevention of uncontrolled positive reactivity insertion	A	RCS overcooling protection	Tur	rbine Trip RT checkback Turbine admission valves	Class 1	F1A	PS	RCS overcooling protection		SIV closure	F1A	PS	Excessive increase in steam flow study	
					x		into the core	~		Full load MF Actuation Front. Syst.	W isolation (4SG) RT checkback Full load MFW isolation valves	Class 1	F1A	PS		Full load M Actuation Front. Syst.	RT checkback Full load MFW isolation valves	F2	SAS	-	
Inadvertent closure of one / all main steam		1 MSIV: 1.8.10 ⁻² All MSIV:	14.4.7		x		Transfer heat from the reactor		Heat removal by Steam	Actuation Front. Syst.	MSRT	Class 1	F1A	PS	Heat removal by Low Head	dise Actuation Front. Syst.	Manual PDS	F2	SAS	Sequences of primary bleed and feed	
isolation valves		2.10 ⁻³		Heat removal	x		coolant to the ultimate heat sink	A	Generators - Emergency shutdown mode	EFW actuat Actuation Front. Syst.	tion (1 train) + SG SG L EFWS injection lines & storages	Class 1	F1A	PS	Emergency Core Cooling System (ECCS)	Actuation Front. Syst.	IS] in cold leg Manual MHSI + LHSI Stop - Manu	F1B	SAS	detailed in case of Total Loss Of FeedWater RRC-A	
					x		Desugat the failure of limit the									Activ. & Elec Front. Syst.	Manual Class 2	F1B	SAS		
				Other	x		Prevent the failure or limit the consequences of failure of a structure, system or component whose failure could cause the impairment of a safety function	A	Essential component protection	Overpres		Class 1	F1A	PS	Essential component protection	SG safety Actuation Front. Syst.	y valves opening Passive MSSV	F1A	-	Secondary overpressure studies of Sub- chapter 3.4.1.5 illustrate	
				Confinement	x		Maintain integrity of the Reactor Coolant Pressure Boundary	A	RCS overpressure protection		Passive	Class 1	F1A	-	RCS overpressure protection	Hot overpr	Passive Class 1	F1A	-	Primary overpressure studies of Sub- chapter 3.4.1.5 illustrate	

UK EPR

PRE-CONSTRUCTION SAFETY REPORT

CHAPTER 14: DESIGN BASIS ANALYSIS

SUB-CHAPTER : 14.7

PAGE : 35 / 58

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (18/29)

			ssificatio	"			SAFETY FUNC			MAIN LINE				DIVERSE LINE
/	Re	ferences			Tra	ansient pl	hases Plant Level Safety Funct	on	Lower Level Safety Function	Safety Functiona	Groups			Lower Lovel Rately Ponsition Safety Functional Groups
	Category	Frequency	PCSR Ref.	Main Safety Function	Cor stat	nt. Safe te state	Based on EPR process a international practice for PWR state	d Safety Cat.	Combination of the Plant Level Safety Function and the conditions of operations (normal, incident, accident)	Item	Safety class	System Req.		Combination of the Plant Level Subjects States States States Communication and the Subjects Communication and the States Communication Communication Communications and Communications Com
Increase in Heat Remo	moval									Reactor trip - auto				
					x		Shutdown and maintain co sub-criticality	A A	Negative reactivity fast insertion	Actuation dP/dt SG L Front. Syst. CRDM	Class 1	F1A	PS	
				Reactivity Control	x		Prevention of uncontrolle positive reactivity insertio		RCS overcooling protection	Turbine Trip Actuation RT checkback Front. Syst. Turbine admission valves	Class 1	F1A	PS	
					x		into the core			Steam line isolation (1SG) Activ. & Elec dP/dt Front. Syst. MSIV	Class 1	F1A	PS	
Frankriske line	PCC-4				x					SG Pressure Control - Cooling Actuation SG P Front. Syst. MSRT	Class 1	F1A	PS	
	0-6/(r.y) <f<10- 4/(r.y)</f<10- 	-	14.5.3	Heat removal	x		Transfer heat from the read coolant to the ultimate he		Heat removal by Steam Generators - Emergency shutdown mode	EFW actuation (1 train) + SG Actuation SG L Front. Syst. EFWS injection line & storages	Class 1	F1A	PS	N/A - diversity is applied to frequent initiating event above 10-3/r.y
					x					Re-alignment of EFWS pump discharge & suction Actuation Manual Front. Syst. EFWS injection line	Class 1	F1A	-	
				Other	x		Prevent the failure or limit consequences of failure o structure, system or component whose failur	a A	Essential component protection	SG Pressure Control - Overpressure protection Actuation SG P Front. Syst. MSRT	Class 1	F1A	PS	
				Confinement	x		Maintain integrity of the Reactor Coolant Pressur Boundary		RCS overpressure protection	Hot overpressure protection Actuation Passive Front. Syst. PSV	Class 1	F1A	-	
				Reactivity Control		x	Shutdown and maintain co sub-criticality	re B	Compensation for shutdown moderator effect	Emergency boron injection into the core - Manual Actuation Manual Front. Syst. EBS	Class 2	F1B	SAS	
						x		в	Heat removal by Steam Generators - Emergency shutdown mode	SG Pressure Control - Cooling Actuation Manual Front. Syst. MSRT	Class 2	F1B	SAS	
Emergency Operating Procedure	All	N/A	All			x	Transfer heat from the read			EFW isolation* Actuation Manual Front. Syst. EFWS injection line	Class 1	F1A	PS	See Appendix A
				Heat removal		x	coolant to the ultimate he sink	B	Heat removal in shutdown mode by Residual Heat Removal system (RHRS)	RCS depressurisation by PZR safety valves Actuation Manual Front. Syst. PSV	Class 2	F1B	SAS	
				Confinement		x	N/A	в		RHR connection and start-up (non-stress) SI signal) Activ. & Elec Front. Syst.	Class 2	F1B	SAS	

* Only the EFWS of the SG aff FeedWater Line Break is isolate the size of the break	ected by the d - whatever

PAGE : 36 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

UK EPR

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (19/29)

PRE-CONSTRUCTION SAFETY REPORT

		Input to clas	ssificatio	n			_	SAFETY FUNCTION	N		MAIN						DIVERSE LINE	
Fault	Re	eferences		Main Safety	Tra	ansient	phases			Lower Level Safety Function		Safety Functional G	iroups			Lower Level Safety Function	Saley Punctional Groups	
description	Category	Frequency	PCSR Ref.	Function	Cont state	t. Saf e stat	e Final se state	Based on EPR process and international practice for PWR	Safety Cat.	Safety Function and the conditions of operations (normal, incident, accident)		Item	Safety class	System Req.		Salaty Extraction and the conditions of generations (normal, incident, accident)	team Surfery Syst class Roap	Suppor
Increase in Heat	Removal		1			1	_											
				Reactivity			x	Shutdown and maintain core sub-criticality	в	Negative reactivity fast insertion	Actuation	Low RCP speed Low RCS loop flowrate	Class 1	F1A	PS			
				Control				Prevention of uncontrolled			Front. Syst. Tu Actuation Front. Syst.	rbine Trip	Class 1	F1A	PS			
							x	positive reactivity insertion into the core	В	RCS overcooling protection	Full load MI Actuation Front. Syst.	FW isolation (4SG) RT checkback Full load MFW isolation valves	Class 1	F1A	PS			
											Actuation	e Control - Cooling Manual	Class 2	F1B	SAS			
Total Loss Of							x		в	Water injection into the RCS	Front. Syst. MHSI in Actuation Front. Syst.	MSRT njection - Auto SIS signal [PZR P] MHSI	Class 1	F1A	PS			
the Cooling Chain leading to a leakage on RCP [RCS]	RRC-A	-	16.3.5					Maintain sufficient Reactor Coolant System water inventory for core cooling				e Control - Cooling SIS signal [PZR P] MSRT	Class 1	F1A	PS		See Appendix A	
pumps seals (state A) TLOCC in state			16.3.11					_			LHSI inje Actuation Front. Syst.	ction diversified Manual LHSI CVCS letdown line	Class 2	F2	SAS			
D				Heat removal			x		В	Prevention of RCS drainage through auxiliary lines	Actuation Front. Syst.		Class 1	F1A	PS			
							x			Heat removal by Steam Generators - Emergency	Actuation Front. Syst.	MSRT	Class 1	F1A	PS			
							x	Transfer heat from the reactor coolant to the ultimate heat sink	в	shutdown mode	EFW actua Actuation Front. Syst.	tion (1 train) + SG SG L EFWS injection lines & storages	Class 1	F1A	PS			
							x			Heat removal from containment by Containment Heat Removal system (CHRS)		WST pool cooling by CHRS Manual CHRS	Class 2	F2	SAS			
				Confinement			x	Limit the release of radioactive material from the reactor containment	в	Containment building isolation	Contain Actuation Front. Syst.	ment isolation Manual Containment isolation valves	Class 2	F1B	SAS			
Loss of one cooling train of the SIS / RHRS in RHR mode (states C & D)	PCC-2 f>10-2/(r.y)	> 1.10 ⁻²	14.3.17	Heat removal	x			Transfer heat from the reactor coolant to the ultimate heat sink	A	Heat removal in shutdown mode by Residual Heat Removal System (RHRS)		out any consequences uarantee heat removal RHR train	- the operat			The diversity	r can be illustrated by the Total Loss of Cooling Chain sec	quences

iky study	Comments
	This part of transient is valid as long as the cooling of MHSI pumps is efficient (-5 minutes). Later the MHSI are lost and the end of the transient is similar to the RRC-A sequences SB LOCA with loss of MHSI. However, in case of TLOCC, there is a need to consider a diverse cooling chaing constituted by the 2 LHSI trains connected to the diverse cooling chain with EVU/SRU. TLOCC in state D relies on the CHRS [EVU] capacities to remove heat with the same features as the one of TLOCC in state A.

SUB-CHAPTER : 14.7

PAGE : 37 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (20/29)

		Input to	classificat	ion					SAFETY FUNCTION	ON		MAIN	LINE				OVERSE LIKE
Fault	R	References		Main Safe	ty	Transie	ent pha	ases	Plant Level Safety Function Based on EPR process and	Safety Cat	Lower Level Safety Function Combination of the Plant Level		Safety Functional C	Groups			Lower Loost Ballery Purcture Solity Reading Content Groups
description	Category	Frequen	cy PCSI Ref.				Safe state	Final state	international practice for PWR	ouldy out.	Safety Function and the conditions of operations (normal, incident, accident)		Item	Safety class	System Req.		Solary AutoBits and the Been Solary Syst California (Second Solari California)
Increase in Hea	at Removal				_	1	1	I		1	1						
				Reactivi				x	Shutdown and maintain core sub-criticality	в	Negative reactivity fast insertion		Reactor trip - auto Mismatch between reactor power and ARE flow	Class 3	F2	RCSL/PS	3
				Control								Front. Syst.	SG L CRDM				
								x	Prevention of uncontrolled positive reactivity insertion into the core	в	RCS overcooling protection		rbine Trip	Class 1	F1A	PS	
								x					of severe accident charge line Manual	Class 2	F2	SAS	
								x					IS] in cold leg Manual	Class 2	F1B	SAS	
Total Loss Of	RRC-A		16.1.3	.3 Heat remo	val			x	Transfer heat from the reactor coolant to the ultimate heat sink	в	Heat removal by Low Head Emergency Core Cooling System (ECCS)	Contain Actuation Front. Syst.	Ment isolation Manual Containment isolation valves	Class 2	F1B	SAS	N/A - diversity is applied to frequent initiating event above 10-3/r.y
FeedWater								x	Sink		Gystelli (2000)	Actuation Front. Syst.	Passive IRWST systems	Class 1	F1A	PS	
								x				Actuation Front. Syst.	Manual MHSI + LHSI	Class 1	F1A	PS	
								x				Activ. & Elec Front. Syst.		Class 2	F1B	SAS	
				Other				x	Prevent the failure or limit the consequences of failure of a structure, system or component whose failure could cause the impairment of a safety function	в	Essential component protection	Overpres	ssure Control - ssure protection SG P MSRT	Class 1	F1A	PS	
				Confinem	ent			x	Limit the release of radioactive material from the reactor containment	в	Containment building isolation	Contair Actuation Front. Syst.	Manual Containment isolation valves	Class 2	F1B	SAS	
								x	Maintain integrity of the Reactor Coolant Pressure Boundary	В	RCS overpressure protection	Hot overpr Actuation Front. Syst.	Passive	Class 1	F1A	-	

UK EPR

ding daily	Comments

UK EPR

PRE-CONSTRUCTION SAFETY REPORT

CHAPTER 14: DESIGN BASIS ANALYSIS

SUB-CHAPTER : 14.7

PAGE : 38 / 58

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (21/29)

		Input to cla	ssificatio	n				SAFETY FUNCTION	ON		MAIN LINE					DIVERSE LINE	
Fault	Re	ferences		Main Safety	Tra	ansient	phases	Plant Level Safety Function Based on EPR process and		Lower Level Safety Function Combination of the Plant Level	Safety Fi	inctional Groups			Lower Level Safety Function Combination of the Plant Lovel	Safaty Functional Groups	Suppo
description	Category Removal	Frequency	PCSR Ref.	Function	Con stat	nt. Safe te stat		international practice for PWR		Safety Function and the conditions of operations (normal, incident, accident)	lte	m Safety class	System Req.		Salah) Function and the continuous of operations (Dermal, moldari, accident)	item Rater Ryst close Rate	
											Reactor trip - au	0					
				Reactivity			x	Shutdown and maintain core sub-criticality	В	Negative reactivity fast insertior	Actuation Low RC Low RC flow Front. Syst. CR	rate	F1A	PS			
				Control				Prevention of uncontrolled			Actuation RT che Front. Syst. Turbine a val	ckback dmission	F1A	PS			
							x	positive reactivity insertion into the core	В	RCS overcooling protection	Full load MFW isolatio Actuation RT che Front. Syst. Full loa isolation isolation	n (4SG) ckback d MFW	F1A	PS			
											SG Pressure Control - Actuation Mai	Cooling Class	2 F1B	SAS			
Total Loss Of							x		в	Water injection into the RCS	Front. Syst. MS MHSI injection - A Actuation SIS signa Front. Syst. MH	uto	F1A	PS			
the Cooling Chain leading to a leakage on RCP [RCS]			16.3.5					Maintain sufficient Reactor Coolant System water inventory for core cooling			SG Pressure Control - Actuation SIS signa	Class	F1A	PS			
pumps seals (state A)	RRC-A		16.3.11								Front. Syst. MS LHSI injection diver Actuation Man Front. Syst. LH	nual Class	? F2	SAS		See Appendix A	
D				Heat removal			x		В	Prevention of RCS drainage through auxiliary lines	Isolation of CVCS letde Actuation SIS signa Front. Syst. CVCS letde	[PZR P] Class	F1A	PS			
							x			Heat removal by Steam Generators - Emergency	SG Pressure Control - Actuation SG Front. Syst. MS	Class	F1A	PS			
							x	Transfer heat from the reacto coolant to the ultimate heat sink		shutdown mode	EFW actuation (1 train	ction lines Class	F1A	PS			
							x			Heat removal from containment by Containment Heat Removal system (CHRS)		0,1	2 F2	SAS			
				Confinement	-		x	Limit the release of radioactive material from the reactor containment	В	Containment building isolation	Containment isola Actuation Mar Eront Syst Contai	tion nual nment	2 F1B	SAS			
Loss of one cooling train of the SIS / RHRS in RHR mode (states C & D)	PCC-2 f>10-2/(r.y)	> 1.10 ⁻²	14.3.17	Heat removal	x			Transfer heat from the reacto coolant to the ultimate heat sink		Heat removal in shutdown mode by Residual Heat Removal System (RHRS)	Transient without any con sufficient to guarantee he	sequences as 2 LHS	rator can actu		The divers	ty can be illustrated by the Total Loss of Cooling Chain s	equences

g study	Comments
	This part of transient is valid as long as the cooling of MHSI pumps is efficient (-5 minutes). Later the MHSI are lost and the end of the transient is similar to the RRC-A sequences SB LOCA with loss of MHSI. However, in case of TLOCC, there is a need to consider a diverse cooling chaing constituted by the 2 LHSI trains connected to the diverse cooling chain with EVU/SRU. TLOCC in state D relies on the CHRS [EVU] capacities to remove heat with the same features as the one of TLOCC in state A.

PAGE : 39 / 58

PRE-CONSTRUCTION SAFETY REPORT

UK EPR

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

DIVERSE LINE Safety Functional Groups ombination of the Safety Functio conditions of o (normal, inciden Supporting study Safety class Syst Req. Safety System class Req. Item Cont. Safe Financial State PCSE Category ergency boron injection into the core - diversified Reactor trip - auto Low RCP speed Low RCS loop flowrate ATWS signal (N-3 rod drop) PCSR Sub-chapter 16.1.3.3.1 - ATWS LOOP High concentrated and high pressure boron injection F2 F1A PS Actuation lass 1 CRDM EBS Front. Syst. Front. Syst. own and maintain c sub-criticality А Reactivity Control Reactor trip - auto Negative reactivity fast insertion F2 SAS Actuation Low RCP speed Front. Sys CRDM Prevention of uncontrolled positive reactivity insertion into the core SG P RT checkback Turbine admission PCC-2 >10-2/(r.y) Actuati Short-term LOOP (<2 hours) x Actuation F1A F1A 6.10⁻² 14.3.6 А RCS overcooling protection Class 1 PS RCS overcooling protection PS Excessive increase in steam flow study MSIV Front. Syst. Front. Syst. valves ning of PCC-3 0-4/(r.y)<f<10 2/(r.y) Long-term LOOP (>2 hours) discharge line Actuation Manual ront. Syst. PDS F1A PS F2 SAS х Class 1 1.10⁻³ Actuation SG P Front, Syst. MSRT 14.4.2 EFW a SIS [RIS] in cold leg F1A PS F1B Actuation SG L Front. Syst. EFWS injection lines & storages ransfer heat from the react coolant to the ultimate heat sink Class 1 Actuation Manual SAS PCSR Sub-chapter 16.1.3.3.4 or 16.1.3.3.3 for electrical supply diversity (see below RRC-A Station Black-out) Heat removal by Low Head Emergency Core Cooling System (ECCS) Heat removal by Steam Generators - Emergency shutdown mode А Front. Syst. MHSI + LHSI RCP stop - Manu Activ. & Elec Manual Front. Syst. RCP UDG-DG start-up F1B SAS EDG start-up Class 1 F1A PS F2 uation LOOP t. Syst. UDG-DG Manual UDG-DG Actuation Front. Syst. consequences of failure of a structure, system or component whose failure build cause the impairment of SG Pressure Control -Overpressure protection SG safety valves opening F1A PS dary overpressure studies of Sub-chapter 3.4.1.5 illustrate F1A А Other Class 1 Actuation Passive Front. Syst. MSSV Actuation SG P Front. Syst. MSRT Maintain integrity of the Reactor Coolant Pressure Boundary Hot overpres sure protection Hot overpr Primary overpressure studies of Sub-chapter 3.4.1.5 illustrate F1A F1A А RCS ove Class 1 Activ. & Elec Passive Front, Syst. PSV Passive PSV ont, Syst. nergency boron injection inte the core - Manual tdown and maintain co sub-criticality Compensation for shutdown moderator effect F1B Reactivity Control SAS в Class 2 Actuation Manual Front. Syst. EBS Heat removal by Steam Generators - Emergency shutdown mode SG Pressure Control - Cooling Emergency Operating Procedure в F1B SAS Class 2 All N/A Actuation Manual Front. Syst. MSRT See Appendix A All ransfer heat from the reac coolant to the ultimate hea sink RCS pressure decrease by Energy discharge from pressurizer x в F1B SAS Class 2 oval in shute x в SAS mode by Residual Heat Removal system (RHRS) Activ. & Elec Manual Class 2 Front Syst RHRS F1B Low RCP speed Low RCS loop flowrate CRDM tdown and maintain sub-criticality в Actuation F1A PS Class 1 Front. Syst. Reactivity Control Prevention of uncontrolled RT checkback Turbine admission F1A PS oositive reactivity insertion into the core в RCS overcooling prot Actuation Class 1 Front. Syst. SAS F1B Class 2 Actuation Manual MSRT EFW header opening Actuation Manual EFWS injection lines F1B Class 2 в Heat removal by Steam Generators - Emergency shutdown mode sfer heat from the rea Front, Syst. & storages coolant to the ultimate heat sink Station Black-out in state A RRC-A 16.1.3.3 F1B SAS Actuation Manual Front. Syst. EFWS injection lines & storages Class 2 N/A - diversity is applied to frequent initiating event above 10-3/r.y в SAS Class 2 F2 Prevent the failure or limit the consequences of failure of a structure, system or component whose failure pould cause the impairment of a safety function F2 PAS Class 3 Othe в F1A PS Class 1 Actuation Front, Syst. SG P Maintain integrity of the Reactor Coolant Pressure Boundary в RCS overpressure protection Actuation Passive Class 1 Front. Syst. PSV F1A PCC-4 10-6/(r.y)<f<10-4/(r.y) Long-term OOP in state C (>2 hours) ansfer heat from the reacto coolant to the ultimate heat sink Heat removal in shutdown mode by Residual Heat Removal System (RHRS) This heat removal is ensured once the EDGs have been aut started - this automatic start is Class 1 14.5.1 А

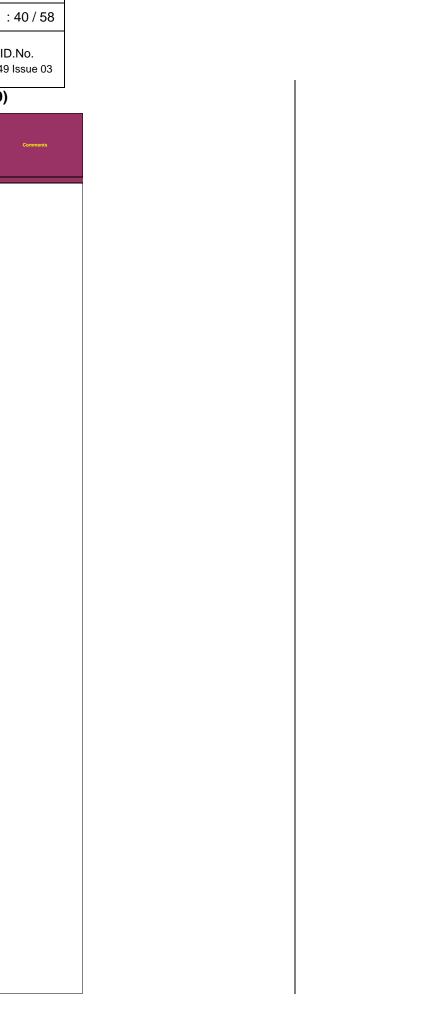
SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (22/29)

Comments	
ATWS are not postulated for PCC-3 and PCC-4 events	
FWS is lost due to the initiating event - no isolation is required.	
he electrical supply of the systems is made the 2h batteries and the 4 EDGs. In case If faiureof the 4 EDGs there are 2 Station lack-out diesels starting the EFVS pumps of trains 1 and 4.	
The overpressure protection is ensured	
The overpressure protection is ensured thanks to the 3 PSVs. It can be demonstrated that no CCF will impair the	
operation of the 3 PSVs at the same time.	
hatever the length of the LOOP, the safety stems actuated are supported by batteries and EDGs allowing	
e electrical supply of the systems is made y the 2h batteries and the 2 Station Black- out diselest starting the EFWS pumps of trains 1 and 4. This heat removal is performed with only two SG after 30 minutes.	
e automatic start-up of the EDGs ensure e heat removal with the LHSI/RHRS trains	



SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (23/29)

		Input to cla	assificatio	on				SAFETY FUNCTION	N		MAIN	ILINE						DIVER	SE LINE			
		References			Transi	sient pha	ISES F	Plant Level Safety Function		Lower Level Safety Function		Safety Functiona	Groups			Lower Level Safety Function	5	ialety Functional	Groups			
NO. Fault description				Main Safety Function		<u> </u>		Based on EPR process and international practice for	Safety Cat.	Combination of the Plant Level Safety Function and the conditions of operations	1	ltem	Safety class	System Req.		Combination of the Plant Level Salety Function and the conditions of operations		Rem	Safety class	Syst Req.	Supporting study	Comments
ATWS	Category	Frequency	Ref.		state	Safe state	state	PŴR		cond ⁱ tions of operations (normal, incident, accident)			Chubb			(normal, incident, accident)			0.000			
							x			Negative reactivity fast insertion	Actuation	SG dP/dt CRDM BLOCKAG	Class 2	F2	PS							
							x	Shutdown and maintain core	в		Emergency Actuation	ATWS signal	Class 2	F2	PS							
								sub-criticality		High concentrated and high pressure boron injection		on of CVCS tank				-						
				Reactivity Control			x				Front. Syst.	ATWS signal CVCS tank urbine Trip	Class 2	F2	PS							
							x	Prevention of uncontrolled positive reactivity insertion	в	RCS overcooling protection	Front. Syst.		Class 1	F1A	PS							
							x	into the core	5	New overcooling protection	Full load M Actuation Front. Syst.	RT checkback Full load MFW	Class 1	F1A	PS							
							x				SG Pressu	re Control - Cooling	Class 1	F1A	PS							
ATWS rod failure - Excessive	RRC-A		16.1.3. ⁻ .1	1							Actuation Front. Syst. EFW actu	MSRT ation (1 train) + SG										
increase in steam flow				Heat removal	•		x	Transfer heat from the reactor coolant to the ultimate heat sink	в	Heat removal by Steam Generators - Emergency shutdown mode	Actuation Front. Syst.	EFWS injection line	Class 1	F1A	PS							
							x				RC	& storages P stop - auto ATWS + SG L	Class 2	F2	PS							
											Front. Syst. SG Pro					-						
							XF	Prevent the failure or limit the consequences of failure of a structure, system or	в		Actuation Front. Syst.	SG P	Class 1	F1A								
				Other			x	component whose failure could cause the impairment of a safety function	в	Essential component protection	SG Pre Overpre	essure Control - essure protection	Class 1	F1A	PS							
NLURE											Actuation Front. Syst.					_						
ROD FA				Confinement			x	Maintain integrity of the Reactor Coolant Pressure Boundary	в	RCS overpressure protection	Hot overp Actuation	Passive	Class 1	F1A	-							
OWING			+								Front. Syst.	PSV										
ATWS rod			16.1.3.																			
A failure - Loss		-	.2	Desp	oite some di	lifference	es in the	e thermal hydraulic transient, t	he systems ir	wolved in the mitigation of the a	ccident are simil	lar to the ATWS Exce	ssive increase	in steam flo	w							
ATWS rod failure - Loss (Offsite Powe		-	16.1.3. ⁻ .3	1 Desp	oite some di	difference	es in the	e thermal hydraulic transient, t	he systems ir	wolved in the mitigation of the a	ccident are simil	lar to the ATWS Exce	ssive increase	in steam flo	w							
Unsite Powe																						
																-						
ATWS rod failure - RCV [CVCS]																		N/A - dive	rsity is applied	1 to frequent	t initiating event above 10-3/r.y	
malfunction th leads to a decrease in th	RRC-A	-	16.1.3. ⁻ .4	1 Desp	oite some di	difference	es in the	e thermal hydraulic transient, t	he systems ir	wolved in the mitigation of the a	ccident are simil	lar to the ATWS Exce	ssive increase	in steam flo	w							
boron concentration the primary	of																					
coolant																						
ATWS rod																						
failure - Uncontrolled RCCA bank	RRC-A		16.1.3. ⁻ .5	1 Desp	oite some di	difference	es in the	e thermal hydraulic transient, t	he systems ir	nvolved in the mitigation of the a	ccident are simil	lar to the ATWS Exce	ssive increase	in steam flo	w							
withdrawal																						
																-						
ATWS PS - Excessive			16.1.3.:	2																		
increase in steam flow	RRC-A	-	.1																			
2																						
ATWS PS - Los Of Main FeedWater	RRC-A	-	16.1.3. .2	132 2																		
ATWS PS - Los	s RRC-A		16.1.3.	2	ara ==	rod by "	une in .	d PT in the DAC T	involue	he mitigation of the sequences a	n cimilee · · ·	open investor the st	nitionite:	o rolete i C								
Of Offsite Pow	er intera		.3	Such ATWS :	ане ттапад	ien nà qu	vərsified	and in the FAS. The systems	des	he mitigation of the sequences a cribed in the fault schedule	re similar to the	ones involved in the	mayauon of ti	e relatêd PC	CC EVENTS							
ATWS PS - RC	v																					
[CVCS] malfunction th leads to a																						
decrease in the boron concentration		-	16.1.3.: .4	2																		
the primary coolant																						
ATWS PS - Uncontrolled	RRC-A		16.1.3.	2																		
RCCA bank withdrawal			.5																			
				-												•						



PAGE : 41 / 58

PRE-CONSTRUCTION SAFETY REPORT

UK EPR

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

Input to cl Safety Functional Groups ver Level Safetv F ombination of the Plant Le Safety Function and the conditions of operations (normal, incident, accident d on EPR process an mational practice for PWR Supporting study Safety System class Req. Safety class Syst Req. Item Cont. Safe Fin state state sta PCSR Ref Manual start-up of the FPCS 3rd train Start-up of a FPCS main train oss of one train Maintain heat removal from fuel stored outside the reactor coolant system but within the site e fuel pool coolir (stem (FPCS) or (supporting syste (state A) PCC-2 f>10-2/(r.y) в Fuel pool heat removal Class 1 F1A PS Fuel pool heat removal F2 SAS Actuation Manual Actuation Manual Front. Syst. FPCS Front. Syst. FPCS Manual start-up of the FPCS 3rd train Start-up of a FPCS main train Maintain heat removal from fuel stored outside the reactor coolant system but within the site Long term LOOP fuel pool cooling aspects (state A) PCC-3 10-4/(r.y)<f< 2/(r.y) F2 в Fuel pool heat removal Class 1 F1A PS Fuel pool heat removal Actuation Manual Actuation Manual Front. Syst. FPCS FPCS Front. Syst. Start-up of a FPCS main train oss of one train one fuel pool coolin ystem (FPCS] or of supporting system (state F) Maintain heat removal from fuel stored outside the reactor coolant system but within the site PCC-3 10-4/(r.y)<f< 2/(r.y) Fuel pool heat removal Class 1 F1A PS N/A - diversity is applied to frequent initiating event above 10-3/r.y x в Manual Actuation Front. Syst. FPCS Automatic isolation of SIS/RHR suction line (only one valve automatically closed isolating the erroneous lining) Manual isolation of the CVCS unloading line F1A Water level in the reactor building transfer compartment F1A Class 1 Actuation Manual Actuation Front. Syst. CVCS Front. Syst. SIS/RHR Fuel pool heat removal tomatic detection of water leve in the spent fuel pool with a setpoint of +18.90 m Water make-up to the fuel pool b Classified Fire Fighting Water Supply System F1A PS F1B Class 1 raining via the RC CVCS] draining line (state E) Maintain heat removal from fuel stored outside the reactor coolant system but within the site Spent Fuel Pool PSA PSA initiator RO 40 ent fuel pool water level f = 1.8.10-3/(r.y) Actuation Actuation Manual A + B Fuel pool heat removal Heat remo Classified Fire Fighting Water Supply System ront. Syst. FPCS Front. Syst. Manual start-up of a FPCS main train F1A Actuation Manual lass 1 Front, Syst. FPCS RB pool drain lines isolation valves manual closing FPCS purification pumps swite off (F2) oluntary draining the reactor buildin pool, Spent Fuel Pool no colated (state D or PSA initiator RO 40 3.0.10-3/(r.y) Spent Fuel Pool PSA Maintain heat removal from fuel stored outside the reactor coolant system but within the site A + B Fuel pool heat removal Class 1 F1A PS Fuel pool heat rem F2 Heat rem ¥ Water level in the spent fuel pool with a setpoint of +18.60 m Actuation Manual Actuation Front. Syst. FPCS Front. Syst. FPCS FPCS purification pumps switch off (F2) FB pool drain lines isolation valves automatic closing Inadequately prepared transfe between the bading pit and the building transform partment (sta A) Maintain heat removal from fuel stored outside the reactor coolant system but within the site PSA initiator RO 40 Spent Fuel Pool PSA Water level in the spent fuel pool with a setpoint of +18.40 m Water level in the spent fuel pool with a setpoint of +18.60 m 1.5.10-3/(r.y) в Fuel pool heat removal F1A PS Fuel pool heat remova F2 lass 2 Actuation Actuation FPCS Front. Syst. Front. Syst. FPCS FB pool drain lines isolation valves automatic closing Fuel pool heat removal F1A PS А Water level in the spent fuel pool with a setpoint of +18.40 m Class 1 Actuation Piping failure on a purification line in the fuel building (state A to F) Maintain heat removal from fuel stored outside the reactor coolant system but within the site 10-4/(r.y)<f< 2/(r.y) PCC-3 N/A - diversity is applied to frequent initiating event above 10-3/r.y FPCS Front. Syst. Siphon-breakers on suction & drainage pipes of FB pool purification lines А Fuel pool heat removal Actuation Passive Front. Syst. FPCS

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (24/29)

Comments
Another diverse line: Analogical measurement of water level in the spent fuel pool (class 2)
+ Manual isolation of SIS/CVCS erroneous lining (class 1)
Another diverse line: Analogical measurement of water level in the spent fuel pool (class 2) + (Manual FPCS purification pumps switch-off (class 3) of Manual closing of the transfer tube isolation valve (class 1 but no redundancy)]
Two other diverse lines: A) Analogical measurement of water level in the spent fuel pool (class 2) + Manual FPCS purification pump switch-off
(class 3) B) Analogical measurement of water level in the spent fuel pool (class 2)

PAGE : 42 / 58

PRE-CONSTRUCTION SAFETY REPORT

UK EPR

Document ID.No.

UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (25/29)

CHAPTER 14: DESIGN BASIS ANALYSIS

		Input to class	ification				SAFETY FUNCTIO	N		MAIN					Diverse une
		References			Transient p	hases	Plant Level Safety Function		Lower Level Safety Function		Safety Functional	Groups			Lowert Lawel Satary Functional Biology Functional Biology
Fault description	Category	Frequency	PCSR	Main Safety Function	Cont. Safe	Final	Based on EPR process and international practice for PWR	Safety Cat.	Combination of the Plant Level Safety Function and the conditions of operations (normal, incident, accident)		ltem	Safety class	System Req.		Consideration of the Liberary Section and Liberary Constraints and Comments and Com
Fuel pool transients			Kei.		State State	State									
											ain lines isolation nanual closing				
Piping failure on a purification line in the reactor building (state E)	PCC-3	10-4/(r.y) <f<1 2/(r.y)</f<1 	^{0.} 14.4.16	Heat removal	x		Maintain heat removal from fuel stored outside the reactor coolant system but within the site	A	Fuel pool heat removal	Actuation Front. Syst.	Water level in the reactor building transfert compartment with a setpoint of +17.90 m	Class 1	F1A	PS	N/A - diversity is applied to frequent initiating event above 10-3/r.y
					x			A	Fuel pool heat removal	Siphon-bre	akers on drainage ool purification lines	-	-	-	
Piping failure on a skimming line in the fuel building (states A to F)	PCC-3	10-4/(r.y) <f<1 2/(r.y)</f<1 	^{0.} 14.4.16	Heat removal	x		Maintain heat removal from fuel stored outside the reactor coolant system but within the site	А	Fuel pool heat removal	drainage pip	op at the suction & bes low level of the mming line Passive FPCS		-	-	N/A - diversity is applied to frequent initiating event above 10-3/r.y
Piping failure on a fuel pool water makeup line in the fuel building (states A to F)	PCC-3	10-4/(r.y) <f<1 2/(r.y)</f<1 	^{0.} 14.4.16	Heat removal	x		Maintain heat removal from fuel stored outside the reactor coolant system but within the site	А	Fuel pool heat removal	Drainage stop	Passive FPCS	-	-	-	N/A - diversity is applied to frequent initiating event above 10-3/r.y
Piping failure on a skimming line in the reactor building (state E)	PCC-3	10-4/(r.y) <f<1 2/(r.y)</f<1 	^{0.} 14.4.16	Heat removal	x		Maintain heat removal from fuel stored outside the reactor coolant system but within the site	A	Fuel pool heat removal	Floating Actuation Front. Syst.	device removal Manual FPCS	-	-	-	N/A - diversity is applied to frequent initiating event above 10-3/r.y
					x			A		Siphon-brea drainage pi Actuation Front. Syst.	akers on suction & ipes of FPCS train Passive FPCS	-	-	-	
					x			В		Main FPCS auto Actuation Front. Syst.	S operating pump omatic trip Water level in the spent fuel pool with a setpoint of +18.0 m FPCS	Class 2	F1B	SAS	
Piping failure on a main cooling train	PCC-3	10-4/(r.y) <f<1 2/(r.y)</f<1 	0. 14.4.16	Heat removal	x		Maintain heat removal from fuel stored outside the reactor coolant system but within the	В	Fuel pool heat removal	Actuation Front. Syst.	S train suction line solation Manual FPCS entation lances ent draining to the	Class 2	F1B	-	N/A - diversity is applied to frequent initiating event above 10-3/r.y
(states A to F)		2()			x		site	В		Actuation Front. Syst.	IRWST Manual FPCS SI injection	Class 1 Class 1	F1A F1A	PS PS	
					x			В		Front. Syst. Fuel pool	MHSI I water make-up Manual Classified Fire Fighting Water	Class 2	F1B	SAS + local actions	
					x		·	в			Supply System a FPCS main train	Class 1	F1A	PS	
					x			A	Fuel pool heat removal	Drainage stop low level of t Actuation Front. Syst.	p at the suction pipe the FPCS third train Passive FPCS	-	-	-	
Piping failure on the					x		Maintain heat removal from	в	Fuel pool heat removal	auto	Water level in the spent fuel pool with a setpoint of +18.0 m FPCS		F1B	SAS	
Piping failure on the third FPCS train (state A)	PCC-3	10-4/(r.y) <f<1 2/(r.y)</f<1 	0 [.] 14.4.16	Heat removal	x		fuel stored outside the reactor coolant system but within the site	В	Fuel pool heat removal	3rd train su Actuation Front. Syst.	Ction line isolation Manual FPCS	Class 2	F1B	-	N/A - diversity is applied to frequent initiating event above 10-3/r.y
					×			В	Fuel pool heat removal	Actuation Front. Syst.	Manual Classified Fire Fighting Water Supply System	Class 2	F1B	SAS + local actions	
					x			в	Fuel pool heat removal		a FPCS main train Manual FPCS	Class 1	F1A	PS	

UK EPR

SUB-CHAPTER : 14.7

PAGE : 43 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

					(SUB	-CHAPTER 14.7	- TAE	BLE 1: FAULT	AND P	ROTECTI		CHEC	ULE .	TABLE: FAULTS AT FULL POWER (26/29)	
		Input to classi	fication				SAFETY FUNCTIO			MAIN					DIVENOS LINE	
Fault description	R	eferences		Main Safety Function	Tran	sient pha	Based on EPR process and international practice for	Safety Cat.	Lower Level Safety Function Combination of the Plant Level Safety Function and the conditions of operations		Safety Functional G	Safety	System		Lower Level Bidely Functional Groups Combination of the Planet Level Subtry Exception and Bin Rem Batery Subtry Exception and Bin Rem Batery Subtry Exception	Comments
	Category	Frequency	PCSR Ref.		Cont. state	Safe I state s	Final <i>PWR</i> state		(normal, incident, accident)			class	Req.		(Interfaction of Conditions) and the second and se	
Fuel pool transients									Π							
					x			A	Fuel pool heat removal	Actuation	Water level in the reactor building transfert compartment with a setpoint of +17.90 m	Class 1	F1A	PS		
Isolatable SIS break (<250 mm) in RHR mode (state E)	PCC-4	10-6/(r.y) <f<10 4/(r.y)</f<10 	14.5.15	Heat removal		x	Maintain heat removal from fuel stored outside the reactor coolant system but within the site	В	Fuel pool heat removal		Water level in the spent fuel pool with a setpoint of +18.0 m	Class 2	F1B	SAS	N/A - diversity is applied to frequent initiating event above 10-3/r.y	
						x		В	Fuel pool heat removal		water make-up Manual Classified Fire Fighting Water Supply System	Class 2	F1B	SAS + local actions		
						x		В	Fuel pool heat removal	Start-up of a Actuation Front. Syst.	a FPCS main train Manual FPCS	Class 1	F1A	PS		
					x			А		MHS Actuation Front. Syst.		Class 1	F1A	PS		
					x			А		Actuation Front. Syst.		Class 1	F1A	PS		
					x			A		compartme	entation lances ent draining to the IRWST Manual FPCS	Class 1	F1A	PS		
Non isolatable small break(<50mm) on a line connected to the primary cooling (state E)	PCC-4	10-6/(r.y) <f<10 4/(r.y)</f<10 	⁴ 14.5.15	Heat removal	x		Maintain heat removal from fuel stored outside the reactor coolant system but within the site	A	Fuel pool heat removal	Reactor bu exhaust lines	ilding floor drain s 1 and 2 automatic solated Water level in the spent fuel pool with a setpoint of +18.9 m RPE	Class 1	F1A	PS	N/A - diversity is applied to frequent initiating event above 10-3/r.y	
						x		В		Main FPCS auto Actuation Front. Syst.	Water level in the spent fuel pool with a setpoint of +18.0 m FPCS	Class 2	F1B	SAS		
						x		в		Fuel pool Actuation Front. Syst.	water make-up Manual Classified Fire Fighting Water Supply System	Class 2	F1B	SAS + local actions		
						x		В		Start-up of a Actuation Front. Syst.	a FPCS main train Manual FPCS	Class 1	F1A	PS		
Loss of the two main trains of the Fuel Pool Cooling System during shutdown for refuelling (state F)	RRC-A	-	16.1.3.1 3	Heat removal			Maintain heat removal from fuel stored outside the reactor coolant system but within the site	в	Fuel pool heat removal	Manual start	-up of the 3rd train Manual	Class 2	F2	SAS	N/A - diversity is applied to frequent initiating event above 10-3/r.y	
							x Maintain heat removal from	В			FPCS -up of the 3rd train	Class 3	F2	SAS		
Station Blackout - FPCS aspects (States E & F)	RRC-A	-	16.1.3.1 3	Heat removal			x Maintain heat removal from fuel stored outside the reactor coolant system but within the site	В	Fuel pool heat removal	Actuation Front. Syst. UDG- Actuation Front. Syst.	Manual FPCS DG start-up Manual UDG-DG	Class 3	F2 F2	-	N/A - diversity is applied to frequent initiating event above 10-3/r.y	

PAGE : 44 / 58

PRE-CONSTRUCTION SAFETY REPORT

UK EPR

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

		Input to c	lassificati	on	SU	JB-(СНА	PTER 14.7 -		E 1: FAULT			ION	SCHE	DUL	E TABLE: F	AULTS A			WE	R (2	7/29)	
Fault	R	References	nassincau	Main Sa	ety	ransien	t phases	Plant Level Safety Function Based on EPR process and	Safety Cat.	Lower Level Safety Function	MAIN	Safety Functional				Lower Lovel Safety Function	Safety	y Functional Grou	ups			Supporting study	Comment
description	Category JS	Frequenc	y PCSR Ref.	Function	on Co sta	ont. Sa ate sta	ife Final ate state	international practice for PWR		Safety Function and the conditions of operations (normal, incident, accident)		Item	Safety class	System Req.		Safety Function and the conditions of operations (normal, incident, accident)		nem		Syst Req.			
					1	x				Negative reactivity fast insertion		tor trip - auto PZR P DNBR	Class 1	F1A	PS	High concentrated and high pressure boron injection		versified	Class 2	F2	PS	ATWS cover	
								Shutdown and maintain core sub-criticality	A		Front. Syst.	CRDM					Front. Syst. Reactor trip	EBS					
				Reactiv Contro												Negative reactivity fast insertion	Actuation Front. Syst.	CRDM	Class 2	F2	SAS		
Spurious ctuation of PZR spray	PCC-2		14.3.1	5	-	x		Prevention of uncontrolled positive reactivity insertion into the core	А	RCS overcooling protection	Actuation Front. Syst.	Irbine Trip RT checkback Turbine admission valves FW isolation (4SG)	Class 1	F1A	PS	RCS overcooling protection	MSIV clos Actuation Front. Syst. Full load MFW iso	SG P C MSIV	Class 1	F1A	PS	Excessive increase in steam flow study	
eading to a rease in RC pressure	f>10-2/(r.y)	4.2.10-3				x					Front. Syst.	RT checkback Full load MFW isolation valves re Control - Cooling	Class 1 Class 1	F1A F1A	PS PS		Opening of seve discharge	ull load MFW blation valves ere accident e line		F2 F2	SAS	SAS order in case of ATWS following PS failure	
				Heat rem		x		Transfer heat from the reactor coolant to the ultimate heat sink	А	Heat removal by Steam Generators - Emergency shutdown mode	Actuation Front. Syst. EFW actua Actuation Front. Syst.	MSRT	Class 1	F1A	PS	Heat removal by Low Head Emergency Core Cooling System (ECCS)	Front. Syst. SIS [RIS] in o Actuation	PDS cold leg		F1B		Sequences of primary bleed and feed detailed in case of Total Loss Of FeedWater RRC-A	
				Othe		x		consequences of failure of a structure, system or	A	Essential component protection	Overpres	ssure Control -	Class 1	F1A	PS	Essential component protection	Front. Syst. SG safety valve	Manual C RCP es opening		F1B F1A	SAS -	Secondary overpressure studies of Sub-	
				Confiner		x		component whose failure	A	Prevention of unacceptable core power distribution	Actuation Front. Syst. Normal Actuation Front. Syst.	SG P MSRT spray isolation PZR P Normal spray valves	Class 1	F1A	PS	Prevention of unacceptable core power distribution	Front. Syst. Normal spray Actuation	MSSV isolation		F1B	SAS	chapter 3.4.1.5 illustrate	
						x				Negative reactivity fast insertion	Reac	tor trip - auto PZR P PZR L	Class 1	F1A	PS	High concentrated and high pressure boron injection	Emergency boron the core - div	injection into versified	Class 2	F2	PS	ATWS cover	
								Shutdown and maintain core sub-criticality	А		Front. Syst.	CRDM					Front. Syst. Reactor trip	EBS					
				Reactiv Contro												Negative reactivity fast insertion	Actuation Front. Syst.	HL P CRDM	Class 2	F2	SAS		
Spurious octuation of ZR heaters eading to an	PCC-2 f>10-2/(r.y)	9.8.10-4	14.3.1	5	;	x		Prevention of uncontrolled positive reactivity insertion into the core	A	RCS overcooling protection	Actuation Front. Syst. Full load M	Turbine admission valves FW isolation (4SG)	Class 1	F1A	PS	RCS overcooling protection	MSIV clos Actuation Front. Syst. Full load MFW iso	SG P MSIV olation (4SG)	Class 1	F1A	PS	Excessive increase in steam flow study	
rease in RC pressure						x x					Actuation Front. Syst. SG Pressur Actuation	RT checkback Full load MFW isolation valves re Control - Cooling SG P	Class 1 Class 1	F1A F1A	PS PS		Front. Syst. Fu iso Opening of seve discharge	plation valves	Class 2 Class 2	F2 F2	SAS SAS	SAS order in case of ATWS following PS failure	
				Heat rem		x		Transfer heat from the reactor coolant to the ultimate heat sink	A	Heat removal by Steam Generators - Emergency shutdown mode	Front. Syst. EFW actua Actuation Front. Syst.	MSRT	Class 1	F1A	PS	Heat removal by Low Head Emergency Core Cooling System (ECCS)	Front. Syst. SIS [RIS] in o Actuation Front. Syst. M RCP stop -	PDS cold leg Manual /HSI + LHSI Manu		F1B	SAS	Sequences of primary bleed and feed detailed in case of Total Loss Of FeedWater RRC-A	
				Othe		x		Prevent the failure or limit the consequences of failure of a structure, system or component whose failure	А	Essential component protection			Class 1	F1A	PS	Essential component protection	Activ. & Elec Front. Syst. SG safety valve	Manual (RCP es opening		F1B F1A	SAS -	Secondary overpressure studies of Sub- chapter 3.4.1.5 illustrate	
k in the eous waste	PCC3 10-4/(r.y) <f<10-< td=""><td>3.10-4</td><td>14.4.10</td><td>Confiner</td><td>nent</td><td>x</td><td></td><td>could cause the imnaiment of Maintain integrity of the Reactor Coolant Pressure Boundary</td><td>A</td><td>RCS overpressure protection</td><td></td><td>Passive</td><td>Class 1</td><td>F1A</td><td>•</td><td></td><td>Hot overpressure</td><td>e protection</td><td>Class 1</td><td>F1A</td><td>-</td><td>PCSR Sub-chapter 3.4.1.5.2.2</td><td></td></f<10-<>	3.10-4	14.4.10	Confiner	nent	x		could cause the imnaiment of Maintain integrity of the Reactor Coolant Pressure Boundary	A	RCS overpressure protection		Passive	Class 1	F1A	•		Hot overpressure	e protection	Class 1	F1A	-	PCSR Sub-chapter 3.4.1.5.2.2	
essing em handling dent ture of	2/(r.y) PCC-4 10-6/(r.y) <f<10- 4/(r.y)</f<10- 		14.5.11	-						т	hese transients	are not detailed from a	thermal hyd	raulic point of	view. Ther	e are discussed in the frame of	radiological consequer	nces Sub-chapter	14.6				
lioactivity- ntaining stems in the clear xiliary ilding	PCC-4 10-6/(r.y) <f<10- 4/(r.y)</f<10- 	< 1.10-4	14.5.13	8																			

UK EPR

SUB-CHAPTER : 14.7

PAGE : 45 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (28/29) MAIN LINE SAFETY FUNCTIO **DIVERSE LINE** Safety Functional Groups Safety Functional Groups ower Level Safety Fun ant Level Safety Fr Combination of the Plant Leve Safety Function and the conditions of operations (normal, incident, accident) Main Safet Function Supp Safety Function and the Safety Function and the conditions of operations (normal, incident, accident Safety class Safety Syst Req. Item Req. ional pra PWR PCS ont. Safe class Category Freque SIS/RHR suction pipe isolation valve automatic closing Water level in the А Fuel pool heat removal Class 1 F1A PS reactor building transfert compartment with a setpoint of +17.90 m Actuation Front. Syst. SIS Main FPCS operating pump automatic trip Maintain heat removal fron olatable SIS brea 10-6/(r.y)<f<10 4/(r.y) uel stored outside the reacto (<250 mm) in RHR mode (state E) PCC-4 14.5.15 Heat r Water level in the F1B SAS N/A - diversity is applied to frequent initiating event above 10-3/r.y х coolant system but within the site В Fuel pool heat removal Class 2 Actuation spent fuel pool with a setpoint of +18.0 m Front. Syst. FPCS Fuel pool water make-up Actuation SAS + loca Manual Classified Fire В Fuel pool heat removal F1B х Class 2 actions Fighting Water Supply System Front. Syst. Start-up of a FPCS main train ¥ В Fuel pool heat removal Class 1 F1A PS Actuation Manual Front. Syst. FPCS MHSI injection F1A А PS Class 1 Actuation Manual Front. Syst. MHSI RB pool overflow lines opening А PS х Class 1 F1A Actuation Manual Front. Syst. FPCS Instrume on lances compartment draining to the IRWST F1A PS Α Class 1 Actuation Manual Front. Syst. FPCS Reactor building floor drain exhaust lines 1 and 2 automatic isolated F1A PS Class 1 on isolatable smal Water level in the Maintain heat removal fron reak(<50mm) on a the connected to the Actuation 10-6/(r.y)<f<1 fuel stored outside the reacto spent fuel pool with a setpoint of +18.9 m PCC-4 14.5.15 Heat remo Fuel pool heat removal N/A - diversity is applied to frequent initiating event above 10-3/r.y 4/(r.y) coolant system but within the primary cooling (state E) site Front. Syst. RPE Main FPCS operating pump automatic trip F1B SAS в Water level in the Class 2 Actuation spent fuel pool with a setpoint of +18.0 m Front. Syst. FPCS Fuel pool water make-up Manual Classified Fire Fighting Water Actuation SAS + loc в Class 2 F1B actions Front. Syst. Supply System Start-up of a FPCS main train в F1A PS ¥ Class 1 Actuation Manual FPCS Front. Syst. Manual start-up of the 3rd train oss of the two mair trains of the Fuel ool Cooling Systen luring shutdown for refuelling (state F) Maintain heat removal from 16.1.3.1 3 fuel stored outside the reactor coolant system but within the Actuation Manual RRC-A F2 SAS в Fuel pool heat removal Class 2 N/A - diversity is applied to frequent initiating event above 10-3/r.y -Heat remova х site FPCS Front. Syst. Manual start-up of the 3rd train х Maintain heat removal from в Class 3 F2 SAS Station Blackout PCS aspects (Stat E & F) Actuation Manual Front. Syst. FPCS uel stored outside the reacto coolant system but within the site 16.1.3.1 RRC-A -Fuel pool heat removal N/A - diversity is applied to frequent initiating event above 10-3/r.y Actuation Manual Front, Syst, UDG-DG в F2 х Class 2

arling study	Comments

SUB-CHAPTER : 14.7

PAGE : 46 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

UK EPR

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 1: FAULT AND PROTECTION SCHEDULE TABLE: FAULTS AT FULL POWER (29/29)

		Input to classification SAFETY FUNCTION MAIN LINE					DMSRGR LBR								
		Re	eferences			Transient phase	S Plant Level Safety Function		Lower Level Safety Safety Functional Groups			Leaver Level Gatery Function Children Courses			
No. Fa				1	Main Safety Function		Based on EPR process and international practice for	Safety Cat.		Item	Safety class	System	C&I platform	Constitutions of the Films Lover Setting Functions and The International Constitutions of the	Comments
		Category	Frequency	PCSR Ref.		Cont. Safe Fir state state	al PWR te		the conditions of operations (normal, incident, accident)	item	class	Req.		constituents (Aspectation)	
Decreas	se in RCS w	vater inventory						Ī		Reactor trip - auto					
							Shutdown and maintain core		Negative reactivity fast	P7P P			50		
						×	sub-criticality	A	insertion	HL P	Class 1	F1A	PS		
					Reactivity Control					Front. Syst. CRDM Turbine Trip					
						x	Prevention of uncontrolled positive reactivity insertion	A	RCS overcooling protection	Actuation RT checkback Front. Syst. Turbine admission valves Full load MFW isolation (4SG)	Class 1	F1A	PS		
						x	into the core			Actuation RT checkback Front. Syst. Full load MFW isolation valves	Class 1	F1A	PS		
						x				SG Pressure Control - Cooling - Auto (MSR) Class 1	F1A	PS		
							Maintain sufficient Reactor	A	Water injection into the RCS	Actuation SIS signal [PZR P] Front. Syst. MSRT MHSI injection - Auto					
at RC	(10cm²) P seals	tbd	tbd	tbd		x	Coolant System water inventory for core cooling			Actuation SIS signal [PZR P] Front. Syst. MHSI (3 pumps)	Class 1	F1A	PS		
	s of one ard train				Heat removal	x		А	Prevention of RCS drainage through auxiliary lines	Isolation of CVCS letdown line (RCS isolation SI sequence) Actuation SIS signal [PZR P] Front. Syst. CVCS letdown valve	n Class 1	F1A	PS		
						x				Front. Syst. CVCS letdown valve SG Pressure Control - Cooling	Class 1	F1A	PS		
						<u>^</u>	Transfer heat from the reactor coolant to the ultimate heat		Heat removal by Steam Generators - Emergency	Actuation SG P Front. Syst. MSRT EFW actuation (1 train) + SG Blowdown	Class 1		F3		
						x	sink		shutdown mode	Actuation SG L Front. Syst. EFWS injection lines &	Class 1	F1A	PS	Covered by the events "Partial loss of core coolant flow (Loss of one reactor coolant pump)", "Forced decrease of reactor coolant flow (four pumps)" and "Small break LOCA (< DN 50) including a break occurring on the extra boration system injection line (states A and B)"	
							Prevent the failure or limit the			SG Pressure Control - Overpressure protection	=)				
					Other	x	consequences of failure of a structure, system or component whose failure	А	Essential component protection	Actuation SG P	Class 1	F1A	PS		
							could cause the impairment of a safety function			Front. Syst. MSRT					
					Confinement	x	Limit the release of radioactive material from the reactor containment	A	Containment building isolation	Containment isolation stage 1 / RCPB Actuation SIS signal [PZR P] Front. Syst. Containment isolation valve	Class 1	F1A	PS		
						x	Shutdown and maintain core sub-criticality	А	Negative reactivity fast insertion	Reactor trip - auto Actuation Low-low loop flow rate in or loop	e Class 1	F1A	PS		
					Reactivity					Front. Syst. CRDM Turbine Trip Actuation RT checkback	Class 1	F1A	PS		
Partial	loss of				Control	x	Prevention of uncontrolled positive reactivity insertion into the core	A	RCS overcooling protection	Front. Syst. Turbine admission valves Full load MFW isolation (4SG) Actuation RT checkback					
core of flow an	coolant d loss of ifeguard	tbd	tbd	tbd						Front. Syst. Full load MFW isolation valves SG Pressure Control - Cooling	Class 1	F1A	PS		
tr						x	Transfer heat from the reactor		Heat removal by Steam	Actuation SG P Front. Syst. MSRT EFW actuation (1 train) + SG Blowdown	Class 1	F1A	PS		
					Heat removal	x	coolant to the ultimate heat sink	A	Generators - Emergency shutdown mode	Actuation SG L Eropt Syst EFWS injection lines &	Class 1	F1A	PS		
					Other	x	Prevent the failure or limit the consequences of failure of a	A	Essential component	SG Pressure Control - Overpressure Actuation SG P		F1A	PS		
					Reactivity		structure, system or Shutdown and maintain core		protection Compensation for shutdown	Front. Syst. MSRT Emergency boron injection into the core - Manual					
					Control	x	Shutdown and maintain core sub-criticality	В	Compensation for shutdown moderator effect	Actuation Manual Front. Syst. EBS	Class 2	F1A	SAS		
						x	Maintain sufficient Reactor Coolant System water inventory for core cooling	в	Water injection into the RCS	LHSI injection in HL Actuation Manual	Class 2	F1B	SAS		
						x	internet y for core county	в	Heat removal by Steam Generators - Emergency	Front. Syst. LHSI SG Pressure Control - Cooling	Class 2	F1B	SAS	See Appendix A	
	rgency rating						_		shutdown mode	Actuation Manual Front. Syst. MSRT MHSI stop (1 train)			040		
Proc	edure	All	N/A	All	Heat removal	x	Transfer heat from the reactor			Actuation Manual Front. Syst. MHSI	Class 2	F1B	SAS		
						x	coolant to the ultimate heat sink	в	Heat removal in shutdown mode by Residual Heat	MHSI injection on large miniflow Actuation Manual	Class 2	F1B	SAS		
							-		Removal system (RHRS)	Front. Syst. MHSI LHSI switch to RHR mode (1 train)					
						x		В		Activ. & Elec Manual Front. Syst. RHRS	Class 2	F1B	SAS		
					Confinement	x	N/A	В	Containment isolation are a	Iready effective due to automatic actuation. In ca the operator can perform the containment is		tomatic actu	ation failed,		

SUB-CHAPTER : 14.7

PAGE : 47 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 2

Fault and Protection Schedule Table – Definitions

Abbreviation	-	Description	<u>Reference</u>	Event annual frequency	Potential Consequences without mitigation (1)
PCC-1	Anticipated Operational Occurrence (AOO)	Plant Condition Category 1	Normal operations	-	-
PCC-2	conditions (PCC-3 to 10 ⁻³ included)	Plant Condition Category 2	lant Condition Category 2 Reference transients 10 ⁻² /(reactor.year) > f		Local loss of cladding integrity Local fuel pellets melting
PCC-3		Plant Condition Category 3	Reference incidents	$10^{-4}/(reactor.year) < f < 10^{-2}/(reactor.year)$	
PCC-4	Accident conditions	Plant Condition Category 4	Reference accidents	10 ⁻⁶ /(reactor.year) < f < 10 ⁻⁴ /(reactor.year)	Global core melting Global loss of cladding integrity Fuel dispersion

Note (1). Consequences of each transient are estimated when cumulating event with SFC (PCC-2, PCC-3 and PCC-4) and LOOP (PCC-3 and PCC-4)



UK EPR

SUB-CHAPTER : 14.7

PAGE : 48 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - TABLE 3

Fault and Protection Schedule Table (Abbreviations)

Abbreviation	Description	ECS code
ACCU	Accumulator	
AO	Axial Offset	
ATWS	Anticipated Transient Whithout Scram	
CHRS	Containment Heat Removal System	EVU
Cont P	High containment pressure	
CVCS	Chemical And Volume Control System	RCV
DNBR	Departure of Nucleate Boiling Ratio	
EBS	Extra Borating System	RBS
EDG	Emergency Diesel Generator	LHP/Q/R/S
EFWS	Emergency FeedWater System	ASG
FB	Fuel Building	
FCD	Fast Cooldown	
FPCS	Fuel Pool Cooling System	PTR
HCPL	High Core Power Level	
HL P	Hot Leg Pressure	
HLPD	High Linear Power Density	
LCO	Limiting Condition of Operation	
LHSI	Low Head Safety Injection	
MFWS	Main FeedWater System	ARE
MFWS LL	Main FeedWater System Low Load	
MHSI	Medium Head Safety Injection	
MSB	Main Steam Bypass	GCT
MSIV	Main Steam Isolation Valve	
MSRIV	Main Steam Relief Isolation Valve	
MSRT	Main Steam Relief Train	VDA
MSSV	Main Steam Safety Valve	
NF	Neutron Flux	
PAS	Process Automation System	
PCD	Partial Cooldown	
PDS	Primary Depressurisation System	
PSV	Pressuriser Safety Valve	
PT	Partial Trip	
PZR	Presuriser	
PZR L	Pressuriser Level	
PZR P	Pressuriser Pressure	
RB	Reactor Building	
RCP	Reactor Coolant Pump	
RCS	Reactor Coolant System	RCP
RT	Reactor trip - auto	
SAS	Safety Automation System	
SBO - DG	Station BlackOut Diesel Generator	LJP/S
SG	Steam Generator	
SG L	Steam Generator Level	
SG P	Steam Generator Pressure	
SIS	Safety Injection System	RIS
SSS	Start-up and Shutdown System	AAD
SSSS	Stand Still Seal System	DEA
TT	Turbine Trip	



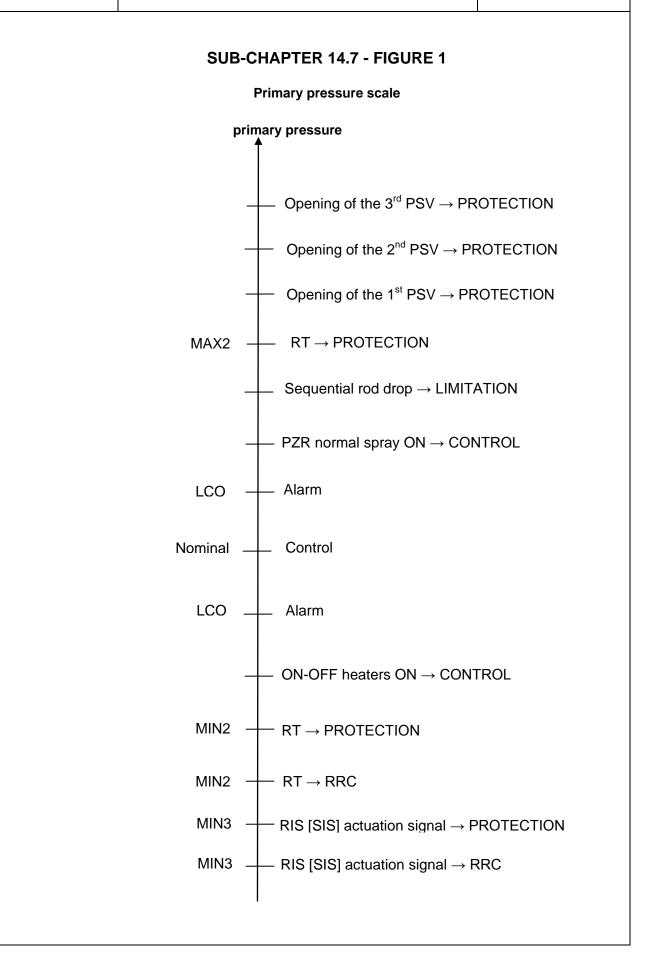
UK EPR

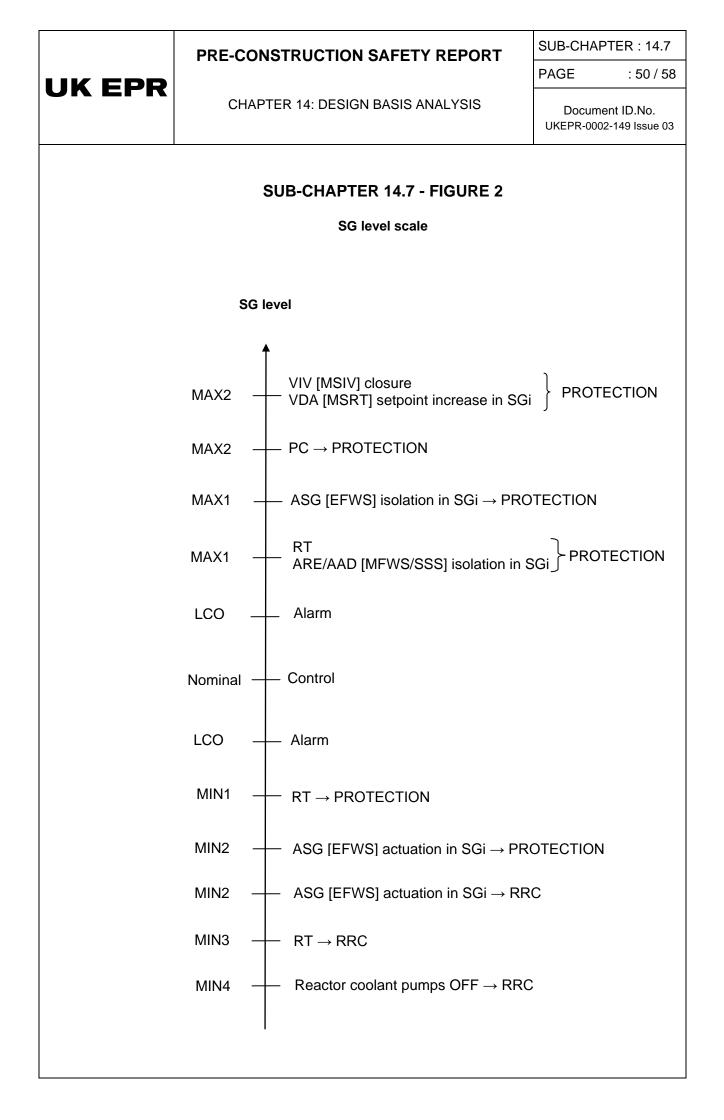
SUB-CHAPTER : 14.7

PAGE : 49 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03





SUB-CHAPTER : 14.7

PAGE : 51 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 - APPENDIX 1

Diversity in Emergency Operating Procedure

This appendix assesses the diverse means available to reach a stable state from the controlled state for all the frequent faults. The controlled state is characterised by short-term heat removal capacity, core sub-criticality and stable core coolant inventory. Hence, the starting point of the analysis is that the controlled state has been reached following the postulated initiating event (PIE) and that no failure of any system has occurred up to that point, other than the system leading to the PIE. Consequently, the three main safety functions, i.e. reactivity control, heat removal and containment, are already ensured – notably the confinement of radioactive materials.

The following analysis first explains the necessary steps to connect to the RRA [RHRS] and then reviews all the frequent events, by event family, to perform the demonstration of diversity. As the emergency operating procedures described in the PCC fault analyses correspond to the safe path, the analysis intends to demonstrate that the feed and bleed procedure is adequate to provide the diversity of the safe path. Subsequently, the objective is not necessarily to demonstrate a safe shutdown state on RRA [RHRS] but it is to achieve a long-term non-hazardous stable state, in which the core is sub-critical, residual heat is removed by primary or secondary systems and off-site radioactive discharges remain acceptable.

A.1. - RRA [RHRS] Connection

The RRA [RHRS] connecting conditions are reached when the reactor coolant system hot leg temperature is lower than 180°C and the hot leg pressure is lower than 32 bar abs.

Four actions must be performed to reach the safe shutdown state from the controlled state:

- RCP [RCS] boration to ensure the core is sub-critical as the temperature and the pressure in the reactor coolant system decrease to reach RRA [RHRS] connecting conditions
- RCP [RCS] depressurisation
- RCP [RCS] cooldown
- Connection to the RRA [RHRS].

The analysis is performed for the frequent postulated initiating events (PIEs).

The operational system used to perform the boration is the RCV [CVCS]. It is Class 3 and therefore cannot be credited in the safety analyses. The RBS [EBS] is the safety classified means of performing the boration to ensure long-term sub-criticality. Should the RBS [EBS] fail, the boration can be performed by a combination of Class 2 systems. For instance, boration can be performed by the bleed and feed procedure, which uses the safety injection system RIS [SIS] and the severe accident discharge lines.

The operational system used to perform the depressurisation of the reactor coolant system is the normal or the auxiliary spray. The depressurisation of the reactor coolant system can also be performed by the safety classified pressuriser safety valves (PSV). Should the pressuriser safety valves fail, the depressurisation of the reactor coolant system can be performed by the Primary Depressurisation System (PDS). However, the PDS actuation requires the use of the RIS [SIS] to compensate for the flow lost through the PDS and to maintain the RCP [RCS] inventory.

UK EPR

SUB-CHAPTER : 14.7

PAGE : 52 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

The cooldown of the reactor coolant system is performed during normal operation by the main steam bypass. The safety classified means to cooldown the reactor coolant system are the VDAs [MSRT]s. Should they fail, the bleed and feed procedure is actuated if the plant situation cannot be stabilised without the VDA [MSRT]s.

The connection to RRA [RHRS] can be performed only if the LHSI pumps are available, as one LHSI train is necessary to ensure the residual heat removal. Should the LHSI pumps not be available, the residual heat can be removed via the steam generators fed by the ASG [EFWS] and using the VDA [MSRT]s. MHSI may be required to maintain the reactor coolant system inventory.

The use of a diverse line may not always be necessary as the plant can be maintained in a controlled state. In particular, this is true in cases where:

- the automatic actions mitigate the PIE, or
- the integrity of the reactor coolant system and the secondary side are not impaired so that their inventories can be maintained after a controlled state is reached.

In these cases, the residual heat is removed by the secondary side in the long term because the steam generator water inventory is high and the reactor coolant system inventory is stable. Typically, the case of a spurious reactor trip falls into this category and is not analysed here any further.

The water volume in the ASG [EFWS] tanks provide sufficient inventory to ensure heat removal for 24 hours at hot shutdown. The ASG [EFWS] tanks can be refilled with water during that time, via the JAC (fire fighting water supply) system.

A.2. - Frequent postulated initiating events

UK EPR

Frequent PIEs are analysed in the following sections in the light of the arguments provided above to demonstrate that a suitably classified diverse line exists to bring the plant to a long-term non-hazardous stable state.

A.2.1. - Increase in RCP [RCS] inventory

The postulated initiating event considered is:

• RCV [CVCS] malfunction causing an increase in reactor coolant inventory

For this event, the diverse line is not necessary as the plant is in a stable state after mitigation of the initiating event by automatic actions, such as isolation of the RCV [CVCS] charging line on high pressuriser level.

In a similar manner to the situation after a reactor trip, the plant is stabilised and can subsequently be maintained in a long-term stable state.

A.2.2. - Decrease in RCS inventory

The postulated initiating events considered are:

- RCV [CVCS] malfunction causing decrease in reactor coolant inventory (state A)
- Inadvertent opening of a pressuriser safety valve

SUB-CHAPTER : 14.7

PAGE : 53 / 58



CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

• Small break (not greater than DN 50) including a break occurring on the Extra Boration System injection line (State A)

In the case of the RCV [CVCS] malfunction, the initiating event is mitigated by automatic actions, such as letdown isolation. The plant can remain in the hot shutdown condition in the long term, even in the event of failure of a system needed to reach the safe shutdown state. Moreover, reaching the RRA [RHRS] connecting conditions under these conditions is bounded by the SB LOCA case.

The case of the inadvertent opening of a pressuriser safety valve is similar to that of the SB LOCA in the phase from the controlled state to the safe shutdown state since at that stage, the PSV opening discharges steam in a similar manner to the SB LOCA case.

Therefore, the analysis is carried out for the case of the SB LOCA. The controlled state is reached when the MHSI flow compensates for the break flow rate and the RCP [RCS] inventory is stable. This ensures sufficient boration in the reactor coolant system. The table below presents the main and diverse lines of the different stages necessary to reach the safe shutdown state.

	Main line	Diverse line
RCP [RCS] boration	Emergency boron injection into	RIS [SIS] + PDS
	the core – Manual	
RCP [RCS] cooldown	SG Pressure Control – Cooling	Not necessary
	(VDA [MSRT])	
RRA [RHRS] connection	Stop MHSI (1 train) - manual	No diversity
RRA [RHRS] connection	LHSI switch to RHR mode	MHSI + EVU [CHRS] +
	(1 train)	VDA [MSRT] + ASG [EFWS]

Main and Diverse Lines to Reach Safe Shutdown State

A.2.3. - Increase in heat removal

The postulated initiating events considered are:

- Feedwater malfunction causing a reduction in feedwater temperature
- Feedwater malfunction causing an increase in feedwater temperature
- Excessive increase in steam flow
- Inadvertent opening of a SG relief train (state A)

For the feedwater malfunction events, as soon as the initiating event is mitigated, by reactor trip and full load main feedwater isolation, the plant is stabilised. The transfer to the safe shutdown state is bounded by the excessive increase in steam flow event.

The inadvertent opening of a SG relief train is mitigated by the closure of the main steam relief train control valve. The plant is then stabilised and heat can be removed by the remaining VDA [MSRT]s. The transfer to the safe shutdown state is performed in the same way as other events in which the integrity of the reactor coolant system or the steam lines is not impaired.

The table below presents the main and diverse lines used to reach a safe shutdown state.

SUB-CHAPTER : 14.7

PAGE : 54 / 58

UK EPR

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

	Main line	Diverse line
RCP [RCS] boration	Emergency boron injection into the core - Manual	RIS [SIS] + PDS
-	Low Load ARE [MFWS] isolation (4 SGs) – manual	Not necessary
RCP [RCS] cooldown	SG Pressure Control – Cooling (VDA [MSRT])	RIS [SIS] + PDS
-	Steam line isolation (1 SG) – auto	No diversity
RCP [RCS] depressurisation	RCP [RCS] depressurisation by pressuriser safety valves	RIS [SIS] + PDS
RRA [RHRS] connection	RRA [RHR] connection and start-up (no SI signal)	VDA [MSRT] + ASG [EFWS]

Main and Diverse Lines to Reach a Safe Shutdown State

A.2.4. - Decrease in heat removal

The postulated initiating events considered are:

- Turbine trip
- Loss of condenser vacuum
- Loss of normal feedwater flow
- Small feedwater system piping failure
- Inadvertent closure of one or all main steam isolation valves

The turbine trip is bounded by the loss of condenser vacuum. The latter event leads to a reactor trip. Under these conditions, the plant can remain in this hot shutdown state as long as boration is performed and water is provided to the steam generators.

The inadvertent closure of one or all VIV [MSIV]s event leads to a similar scenario with the additional isolation of the steam generators. After reactor trip, the plant can remain in the hot shutdown state as long as water is provided to the steam generators.

The bounding event is the loss of main feedwater due to the lower steam generator inventory. Regarding the loss of main feedwater, if the RBS [EBS] is unavailable, the plant is stabilised by the use of the ASG [EFWS] and VDA [MSRT]. The transfer to the safe shutdown state is not necessary as the ASG [EFWS] tank can be supplied with additional water to remove the heat from the reactor coolant system.

Should the PSVs fail, the increase in RCP [RCS] heat is removed by the secondary side as demonstrated by the analysis of closure of the 4 VIV [MSIV]s without PSV in the short term. In the long term, as the failure is postulated on the PSVs, the RCP [RCS] heat can be removed by the ASG [EFWS] and the VDA [MSRT]s. The plant is stabilised in this configuration. The same is true if there is a failure on the LHSI (RHR). The plant is stabilised in a non-hazardous stable state and maintenance can be performed on the equipment.

The table below presents the main and diverse lines used to reach a safe shutdown state.

SUB-CHAPTER : 14.7

PAGE : 55 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

	Main line	Diverse line
RCP [RCS] boration	Emergency boron injection into the core – Manual	RIS [SIS] + PDS
RCP [RCS] cooldown	SG Pressure Control – Cooling (VDA [MSRT])	RIS [SIS] + PDS
RCP [RCS] depressurisation	RCP [RCS] depressurisation by pressuriser safety valves	RIS [SIS] + PDS
RRA connection	RHR connection and start-up (no SI signal)	VDA [MSRT] + ASG [EFWS]

Main and Diverse Lines to reach a Safe Shutdown State

A.2.5. - Electrical power supply fault

UK EPR

The postulated initiating event considered is:

• Short-term loss of off-site power (LOOP)

This case is similar to those identified above, as the short-term LOOP leads to a decrease in heat removal. Therefore, the table in section A2.4 above presents the main and diverse lines used to reach a safe shutdown state.

Moreover, the additional failure that can be combined with the LOOP is the loss of the EDGs. It is demonstrated in PCSR Sub-chapter 16.1 that, in the event of Station Black Out, the safe shutdown state can be reached. Additional details are provided below.

To reach the safe shutdown state, the systems used must be supplied by power in the long term. This is true for:

- RBS [EBS]
- ASG [EFWS]
- RIS [SIS]

The VDA [MSRT]s and PSVs (solenoid pilots) are supplied by two-hour batteries.

Moreover, the two pilots of the third PSV are supplied by electrical divisions 1 and 4, which are supplied by Ultimate Diesel Generators (UDGs). The two pilots must open to actuate the safety valve.

Similarly, the main steam relief control valves of steam lines 1 and 4 are supplied by UDGs.

The LOOP leads to the loss of the reactor coolant pumps, Main Feedwater System (ARE [MFWS]) and turbine trip. Therefore, the ASG [EFWS] and VDA [MSRT]s are necessary to mitigate the event. The heat exchange in the steam generators ensures that the reactor coolant flows by natural circulation due to the temperature difference between the core and the steam generators. Therefore, heat removal is ensured as long as the water inventory in the steam generator is sufficient. The plant can be stabilised in the hot shutdown state.



PAGE : 56 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

A.2.6. - Steam generator tube rupture

UK EPR

In the case of steam generator tube rupture, the controlled state is reached when the leak is compensated by RCP [RCS] water make-up. In the fault studies, SGTR scenarios are demonstrated up to the end of the short-term phase where the SGTR leak flowrate is terminated by establishing a pressure balance between the RCP [RCS] and the affected SG (SGa).

The plant can remain in this condition in the long term, without further actions. Boration has been performed by the RIS [SIS], or the RCV [CVCS] if it is operational, which is more onerous because it prevents RIS [SIS] actuation.

The reactor coolant system inventory is stable due to the RCV [CVCS] or the RIS [SIS] and three steam generators contribute to the residual heat removal.

Radioactive releases are stabilised by isolation of the affected steam generator. If operational systems are available, they can be used to perform their functions. Therefore, the plant can remain in a long-term stable state. Cooldown occurs without intervention in the steam generators due to heat losses and causes the temperature of the reactor coolant system to reduce naturally, allowing the possibility of repairing the impaired systems.

A.2.7. - Reactivity transients

The postulated initiating events considered are:

- Uncontrolled RCCA bank withdrawal at power
- Uncontrolled RCCA bank withdrawal from Hot Zero Power (HZP)
- RCCA misalignment up to control rod drop
- Start-up of an inactive reactor coolant loop at an incorrect temperature
- RCV [CVCS] malfunction that results in a decrease in boron concentration in the reactor coolant
- Uncontrolled single RCCA withdrawal

These events lead to a reactor trip and do not impair the integrity of the reactor coolant system and the secondary side so that their inventories can be maintained after the controlled state is reached. Therefore, the non-hazardous stable state can be maintained in the long term.

A.3. - Conclusions

The use of diverse means to reach the long-term non-hazardous stable state has been demonstrated, when necessary, for all the frequent initiating events. The feed and bleed procedure is used in most cases to ensure depressurisation, cooldown and boration. In the other cases, the plant can remain in a long-term non-hazardous stable state.

<u>Note</u>: Class 1 manual actions with F1A architecture requirements are not required to reach the safe shutdown state. If they are provided to reach the safe shutdown state, it is due to their implementation in order to reach the controlled state in the following PCCs: steam line break, feedwater line break, piping failure on a main cooling train (states A to F).

UK EPR

SUB-CHAPTER : 14.7

PAGE : 57 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

<u>Note</u>: Since the initiating event frequencies for the "loss of support systems" events have not yet been determined, the diverse line for the Emergency Operating Procedures is not analysed in this revision of the Fault Schedule.

SUB-CHAPTER : 14.7

PAGE : 58 / 58

CHAPTER 14: DESIGN BASIS ANALYSIS

Document ID.No. UKEPR-0002-149 Issue 03

SUB-CHAPTER 14.7 – 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. LIST OF INITIATING EVENTS

1.2. NSSS DESIGN CONDITIONS (PCC EVENTS)

[Ref-1] Prouillac. Justification of the internal events list for the design conditions of the NSSS. Fratec 01 Revision E. AREVA. June 1980. (E).

2. JUSTIFICATION OF THE COMPREHENSIVENESS OF FAULT PROTECTION

2.3. DEFENCE LINES

UK EPR

2.3.2 Main defence line (protection)

[Ref-1] P. Martinet. Reactor Trip Concept. NLE-F DC 124 Revision B. June 2008. AREVA. (E).

3. PROTECTION SYSTEM I&C ARCHITECTURE

3.1. SAFETY FUNCTIONS

[Ref-1] L. Carfantan. EPR UK - Definition of P/S I&C functions. NEPR-F DC 469 Revision A. April 2009. AREVA. (E).