UK EPR	Title: PCSR – Sub-Chapter 8.6 – Prevention and Protection against Common Cause Failure
	UKEPR-0002-086 Issue 01

Total number of pages: 24	Page No.: I / IV
Chapter Pilot: E. PILOQUET *Name/Initials* ER Piloquet *Date* *17-10-2012*	
Approved for EDF by: A. MARECHAL *pp. F. BRISSE* *Name/Initials* FBrisse *Date* *17-10-2012*	Approved for AREVA by: G. CRAIG *Name/Initials* G Craig *Date* *17-10-2012*

REVISION HISTORY

Issue	Description	Date
00	First issue.	30-03-2011
01	Consolidated PCSR update: - References listed under each numbered section or sub-section heading numbered [Ref-1], [Ref-2], [Ref-3], etc - Minor editorial changes - Clarification of text (§2.2, §3, §6.1, §6.3) - Section 5 (Human factors) restructured for consistency with report 17074-709-000-RPT-0002, Issue 05 (CAE Document); rearrangement of existing material under §5.1 (General), §5.2 (Design, maintenance and operation) & §5.2.1 (Documentation and human resources); content of previous §5.2 deleted; addition of new §5.2.2 (Control of access), §5.2.3 (Provision of interlocks), §5.2.4 (Operator interfaces) and §5.2.5 (Procedures) - Content of §6.2.4 (insulation co-ordination) deleted and transferred to Sub-chapter 8.4 §3.3; cross-reference to Sub-chapter 8.4 added - Section 6 (Availability …) restructured for consistency with report 17074-709-000-RPT-0002 Issue 05; new material added under existing §6.2.1, §6.2.2, §6.2.3; addition of new §6.2.5 (Frequency transients circa 50 Hz), §6.2.7 (Harmonics), and §6.2.8 (PSA Reliability data); previous §6.3 & §6.3.1 retitled and moved to new §6.2.6 (Fast transients) and new material added; addition of new §6.3 (Segregation, electrical isolation and separation) with cross-reference to Sub-chapter 8.4, new §6.4 (Diversification in design), §6.5 (Prevention of cascading failures between levels). - Reference to the PSA requiring diversity of switchboard control voltage supplies deleted from §6.4.1 (technical correction). Continued on next page	17-10-2012

REVISION HISTORY (Cont'd)

Issue	Description	Date
01 Cont'd	Consolidated PCSR update: - Section 7 restructured \$7.1.1 to §7.1.4 renumbered as §7.1 to §7.4. New material added under \$7.4 (PECS and Software Reliability) for consistency with report 17074-709-000-RPT-0002 Issue 05. - Content of previous §7.2, §7.3 and §7.3.1 to §7.3.1 moved to new §6.3, §6.4.1 and §6.4.2 to §6.4.4 respectively	

For information address:

AREVA NP SAS
Tour AREVA
92084 Paris La Défense Cedex
France

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

TABLE OF CONTENTS

SUB-CHAPTER 8.6 – PREVENTION AND PROTECTION AGAINST COMMON CAUSE FAILURE

1. DEFINITION

Common Cause Failures (CCF) are failures on demand or during a system mission period that could affect and make several items of equipment or components within the same system or with the same function simultaneously unavailable, where the failures are due to the same cause (see section 3.3 of Sub-chapter 15.1).

Common Cause Failures include failures of equipment due to errors in design, manufacture, installation or operation. CCF applies to groups of redundant equipment items operating under similar conditions.

2. IMPLEMENTATION OF PREVENTION AND PROTECTION AGAINST COMMON CAUSE FAILURE

2.1. INTRODUCTION

The sections below set out the arguments and evidence corresponding to a set of safety requirements which have been specified for Common Cause Failure.

They define all the conditions taken into account in terms of the prevention of, and protection against, CCF to meet all the safety requirements.

2.2. PROTECTION SCOPE

Protection against CCF is considered for events resulting from:

- external hazards;
- internal hazards;
- normal voltage and low frequency range phenomena (slow transients: e.g. Forsmark, Olkiluoto 1; short circuit current ($I_{Short\ Circuit}$) , voltage dips, harmonics,…); over-voltage and high frequency range phenomena (fast transients); diversity; and the independence;
- human factors in the design (component or system), and human error in maintenance and in operation; and
- component failure due to ageing or manufacturing fault.

2.3. GENERIC CLAIMS

The risk of Common Cause Failure in the design, manufacturing and maintenance of the nuclear power plant is minimised.

2.4. GENERIC ARGUMENTS

A strategy is implemented to minimise the risk of Common Cause Failure in the design of electrical systems. This strategy is based on a number of arguments:

Argument 1: To segregate one safety division, safety classified redundant equipment and their support systems from the other safety redundant division and equipment.

Chapter D 7000 of the AFCEN RCC-E code [Ref-1] specifies the physical and electrical separation of electrical equipment including electrical defects or electrical disturbances.

Argument 2: To select robust equipment based on operating experience feedback from French and international NPPs.

Argument 3: To prove equipment reliability.

Argument 4: To diversify equipment and support systems involved, if required to achieve the reliability goals (see Chapter 15); within GDA this covers the Emergency Diesel Generators (EDGs) and Ultimate Diesel Generators (UDGs, also known as Station Blackout (SBO) diesel generators), batteries and smart devices.

Argument 5: To mitigate the events contributing to a Common Cause Failure (defence in depth).

3. EXTERNAL HAZARDS

The design of the EPR electrical distribution must be robust when taking into account the occurrence of events resulting from external hazards.

The external hazards to be considered are defined in Sub-chapter 13.1 and include:

- earthquakes;
- aircraft crash;
- hazards associated with the industrial environment and transport routes (external explosion, off-site fire, movement of toxic or corrosive gases);
- external flooding;
- extreme weather conditions (snow and wind, wind generated missiles, low ambient temperatures, icing and frazil ice, high ambient temperatures, drought); and
- lightning and electromagnetic interference.

The reduction of the risk of CCF due to external hazards is based on the segregation between safety buildings, divisions and functions and/or on the design and qualification of equipment to withstand the hazard.

Sub-chapter 13.1 describes the modes of protection implemented against CCF at the generic design stage.

The common mode failure analysis, performed after plant completion, provides final confirmation of plant robustness against events resulting from external hazards.

4. INTERNAL HAZARDS

The design of the EPR electrical distribution must be robust when taking into account the occurrence of events resulting from internal hazards.

The internal hazards considered are defined in Sub-chapter 13.2 and include:

- pipework leaks and breaks;
- failure of tanks, pumps and valves;
- internal missiles;
- dropped loads;
- internal explosions;
- fire; and
- internal flooding.

The reduction of the risk of CCF due to internal hazards is based on the segregation between safety divisions and functions.

Sub-chapter 13.2 describes the modes of protection implemented against CCF at the generic design stage.

The common mode analysis, performed after plant completion, provides final confirmation of plant robustness against events resulting from internal hazards.

5. HUMAN FACTORS

5.1. GENERAL

The design of the EPR electrical distribution must be robust against human errors.

The Level 1 Probabilistic Safety Assessment (PSA) model has identified the equipment and components for which human errors can lead to CCF.

CCF due to human errors is considered in Sub-chapter 18.1 and is related to the equipment and components identified in the PSA.

Sub-chapter 18.1 states that human factors are given due consideration during the design and during all phases and modes of plant operation including normal, abnormal and emergency conditions, testing and maintenance. Particular emphasis is given to design and operating experience.

Sub-chapter 18.1 presents the framework of the Human Factors Engineering (HFE) and considerations associated with:

- the generic design (GDA) stage;
- the detailed design stage; and
- the maintenance and operation stages.

The Human Factors Engineering (HFE) programme is focussed on safety related issues to take advantage of human capabilities and to minimise both the potential for human errors and the impact of those errors on the plant.

Task analysis of safety related human based actions is carried out to ensure that human based safety claims are feasible and fully substantiated. PCSR Sub-chapter 18.1 describes how this analysis work underpins the claims made on human based safety actions. The analysis is applied to post-fault recovery actions and pre-fault activities such as maintenance that could lead to the failure of safety related equipment. This analysis will apply to any risk significant actions that have been identified in relation to electrical systems.

The objective of analysing the activities is to improve the quality of the intervention by maintenance and operational personnel, and to reduce the potential for human error and inadequate action where safety is concerned.

5.2. DESIGN, MAINTENANCE AND OPERATION

5.2.1. Documentation and Human Resources

In the electrical design framework, the objectives of the HFE programme are:

- to define the general and detailed specifications for use by personnel to design, operate and maintain the installation equipment and plant systems; and
- to evaluate the choices made in the initial reference design.

During the basic engineering design phase, the prevention of CCF relies upon design specifications from engineering documents applicable to the design, construction and start-up of electrical systems using electrical power supplies which are specified for each project or contract, for example:

- engineering method related documents are used to fix the common engineering rules designed to ensure that studies remain coherent;
- system design manuals detailing the functional specifications of the installation systems;

- building design files detailing the functional specifications of the buildings housing the installation;
- engineering methodology and design doctrine (e.g. equipment technical specification, segregation of electrical divisions, cable cross-section calculations, load balance calculations); and
- commissioning and start-up documents setting out the engineering methods and implementation rules for system and equipment testing (e.g. standard test guidelines, test procedures).

Prior to the detailed design, the following types of guidelines or procedures are established:

- guidelines to define the contract technical appendices; and
- design engineering and project procedures.

At the generic design stage, chapter C 1200 of the AFCEN RCC-E code [Ref-1] describes the basic specification for the engineering documents above.

At the detailed design stage, the engineering documents are available. The detailed project engineering procedures comply with the overall requirements.

During site licensing, engineering documents and detailed project engineering procedures are consolidated.

The electrical engineering process sets up generic specifications providing the rules, conditions and technical options used to size essential electrical equipment and presents the principles for coordinating the characteristics of nuclear power plant electrical equipment with the rules governing the design of electrical systems. This gathers together numerous items of equipment required to fulfil the various functions covering:

- the coordination of the characteristics of electrical equipment used in plant power generation and distribution to plant auxiliaries, and in particular to safety-related auxiliaries; and
- applicable rules when verifying the availability of safety-class equipment and the rules governing equipment interchangeability.

At the generic design stage, chapter C 2000 of the AFCEN RCC-E code [Ref-1] describes the basic specification for these electrical engineering documents.

During site licensing, the electrical engineering documents are available following issue by the licensee.

The design processes for equipment specification and layout, described in PCSR Sub-chapter 18.1 and the UK HFE programme, support reliable human performance during activities that could impact on safety. This is achieved via integration of human factors in the design process, and is supported by analysis in order to demonstrate that a systematic approach is adopted for the identification of human based actions that could impact safety and also demonstrate that the risk of human error is considered ALARP.

In operation, the appointment of Suitably Qualified and Experienced Personnel (SQEP) contributes to the reduction of human errors.

At the generic design stage, Sub-chapter 21.2 describes the allocation of skilled and experienced people; the resourcing and SQEP processes of the supporting organisations (EDF, AREVA and AMEC) are described.

Reduction of the risk of CCF from human errors in manufacturing is not specified. The equipment specification defines Reliability, Availability and Maintainability (RAM) requirements which tend to be linked to the safety significance of the equipment.

At the generic design stage, the customer provides the equipment specification which defines the reliability and maintainability objectives.

Human factors are taken into account by suppliers in the manufacturing process of electrical equipment. It is integrated in the development of reliability data provided by the manufacturer to meet the goals required by the equipment specifications.

During site licensing, the maintainability data is supplied to the licensee by the equipment supplier.

5.2.2. Control of access

The design and layout of the UK EPR electrical distribution facilitates operator access in a controlled manner for planned and unplanned maintenance, and minimises potential adverse interactions. Such access controls also apply if the operators need to change system settings as part of the maintenance activities.

A high level of protection against inappropriate actions is provided by access control of the electrical distribution buildings. Local access control to electrical system equipment may then include the use of padlocks and interlocks, etc.

During site licensing, arrangements will be established for access and configuration controls.

5.2.3. Provision of Interlocks

Interlocks prevent commands from being implemented that may cause an unwanted action, or damage to equipment. Local mechanical and electrical interlocks are used to ensure that actions are only allowed if required criteria are met.

The basic design document [Ref-1] provides details for scenarios involving key interlocks.

Part 5 of the SDMs for the LJ, LK, LL, LO and LV systems describe some of these interlocks.

5.2.4. Operator interfaces

Information and control of the electrical system is required by the operator in order to carry out functions in various plant states. The plant is designed to allow remote control from the Main Control Room (MCR) and Remote Shutdown Station (RSS) or local control. The information and control available at each location can vary with some signals and controls only being available at one of the three locations and others being replicated at all locations.

Standard diagrams used as the basis for the design specifications show that the input signals to the control room are sufficiently comprehensive to ensure that electrical equipment cannot be shown as available when it is unavailable.

5.2.5. Procedures

Procedures support reliable human performance during activities that can impact on safety and:

- assist the operating and maintenance staff to interact with the electrical system in all operating conditions;
- are technically accurate, comprehensive, explicit, and easy to use; and
- cover activities associated with plant operations, testing, and maintenance.

The procedures for normal operation (e.g. Normal Operating Procedures, Operating Technical Specifications and Periodic Testing procedures) are described in Sub-chapter 18.2. These include procedures and work instructions to assist with Maintenance, Inspection and Testing activities in compliance with the RAM requirements mentioned in section 5.2.1 of this sub-chapter.

The procedures for abnormal operation (e.g. Emergency Operating Procedures and Operating Strategies for Severe Accidents) are described in Sub-chapter 18.3. These will address the following scenarios specific to the electrical system:

- Loss Of Off-site Power (LOOP) combined with loss of all EDGs, and
- Total loss of all AC sources requiring a severe accident configuration.

6. AVAILABILITY OF THE INTERNAL NETWORK AND ASSOCIATED EQUIPMENT

The availability of an internal network and associated equipment is guaranteed within the specified conditions.

The design of the emergency power sources is robust, based on agreed input data.

6.1. MINIMISATION OF DEMANDS ON EMERGENCY POWER SOURCES

The demands on the emergency power sources are limited due to the independence and reliability of off-site sources, and the supply capability via the on-site turbo-generator power source and the auxiliary off-site source.

At the generic design stage:

- Sub-chapter 8.1 defines the requirements on the auxiliary transmission line ensuring adequate independence of the supply from the main transmission line in case of external hazards (e.g. climatic, seismic conditions, sabotage);
- Sub-chapters 8.1 and 8.3 specify the house load operation after a grid fault and opening of the main switchgear; and
- Sub-chapters 8.1 and 8.3 specify the transfer between off-site sources.

6.2. ROBUST DESIGN OF POWER SOURCES

6.2.1. Current Coordination

The input data (e.g. functional load balances, network short circuit capacity, network maximum voltage, transformers short circuit impedance, the diesel generator current, and motor starting current) are used to carry out short-circuit calculations in compliance with the IEC standard [Ref-1] using an iterative approach which determines or verifies the admissible currents for switchgear and other components.

At the generic design stage:

- the coordination of current levels is specified in chapter C 2200 of the AFCEN RCC-E code [Ref-2];
- a power consumption report will be produced to determine the admissible steady state currents as required by chapter C 2211 of the AFCEN RCC-E code [Ref-2];
- the short-circuit calculations on the network are performed in the calculation of three-phase short circuit currents for High Voltage (HV) and Low Voltage (LV) switchboards [Ref-3]; and
- short-circuit calculations will be produced for the DC networks.

During site licensing, the verification of these calculations should be performed by the licensee.

6.2.2. Protection Selectivity

The coordination of electrical protection enables detection of all faults, wherever they occur within the electrical distribution system and rapid isolation so as to limit the effects on equipment.

The selective protection will ensure that the protective device directly upstream of the fault will be activated to eliminate the fault, leaving the other sections of the network energised and unaffected.

At the generic design stage, the coordination of electrical protection is specified in chapter C 2300 of the AFCEN RCC-E code [Ref-1], parts of which introduce rules for protection selectivity. A report detailing the selective protection of electrical equipment describes the selectivity principles [Ref-2].

During site licensing, the detailed implementation of electrical protection coordination will be performed to reflect the UK EPR design, taking into account operating constraints in different plant states for different power sources (step-down transformer (TS), auxiliary transformer (TA), EDG, UDG and Uninterruptible Power Supplies (UPS)) and the equipment chosen.

As required by chapters C 2331 and C 2342 in the AFCEN RCC-E code [Ref-1] for the non-emergency back-up power supplies HV and LV respectively, the voltage protection systems will trip the relevant circuits after an extended loss of voltage. This is to ensure that automatic equipment takes into account the actual condition of the plant and prevents immediate start-up of equipment when voltage is restored.

6.2.3. Voltage Coordination

The voltage coordination follows the rules in chapter C 2100 of the AFCEN RCC-E code [Ref-1].

The input data (e.g. functional load balances, network short circuit capacity, network minimum voltage, transformer short circuit impedance, internal network minimum voltage and load shedding) is used to assess electrical transients to determine and/or verify the acceptability of electrical auxiliary start-up and operating voltages as defined in chapter D 2314 of the AFCEN RCC-E code [Ref-1].

The considered scenarios are:

- grouped auxiliary unit restart on the TS with turbo-generator (TG) and grid network, or on the TS without TG and grid voltage dips;
- start-up of the most powerful motor on the TA and on the TS;
- grouped auxiliary unit restart on the TA after transfer from the main off-site source to the auxiliary off site source with two cases:
    - PCC events with the safety injection and emergency feed water supplies in service and not;
    - normal operation;
- islanding operation; and
- EDG and UDG reloading transients.

The acceptance criterion is a voltage greater than the minimum voltage within a specified period.

At the generic design stage, the detailed design study [Ref-2] provides the Flamanville 3 (FA3) transient analyses of the conventional island except for the EDG and UDG reloading.

During site licensing the GDA transient analyses will be updated and/or verified, including provision of analyses for EDG and UDG reloading.

Section 3.4 of PCSR Sub-chapter 8.1 addresses actions in response to external disturbances, which could include voltage disturbances at frequencies circa 50 Hz.

Measures for AC under voltage protection are provided by the Generator and Power Transmission Protection System (GPA) [Ref-3] and by detection equipment located in the 10 kV Normal Power Supply System (LGi) [Ref-4] and 10 kV Emergency Power Supply System (LHi) [Ref-5] switchboards.

From section 2 of [Ref-3], a fault in the TG voltage regulation system could cause over voltage from an internal source. This would be detected by the GPA, resulting in an alarm at 1.1 Un after 3 seconds followed by a trip of TG and opening of the Generator transformer circuit breaker at 1.2 Un after 3 seconds. Analysis will demonstrate the ability of the GPA to protect against under and over voltage.

The TG for external over voltage, and the TS and TA tap changers compensate for short duration over voltage; and the equipment is designed to have a suitable margin for credible over voltages.

Analysis will demonstrate the ability of the LGi and LHi switchboards to protect against under voltage.

DC equipment is specified to withstand credible over voltages.

Analysis will demonstrate that all electrical system equipment is capable of functioning during specified normal and exceptional voltage ranges.

6.2.4. Insulation coordination

The insulation coordination is described in Sub-chapter 8.4.

6.2.5. Frequency Transients circa 50Hz

From chapter C 2110 of the AFCEN RCC-E code [Ref-1] the frequency of off-site power supplies is usually very close to the nominal value. In the event of incidents, it could deviate by a few hertz, generally as a reduction in frequency.

Section 3.4 of PCSR Sub-chapter 8.1 addresses actions in response to external disturbances, which could include frequency disturbances. In addition, measures for protection from externally generated under frequency transients are provided by the GPA [Ref-2]. Measures for protection from internally generated over frequency transients are provided by the steam turbine over speed protection.

Analysis will demonstrate the ability of the:

- GPA to protect against externally generated over frequency;
- steam turbine over speed protection to protect against internally generated over frequency;
- electrical system equipment to meet the withstand requirements for a one off internally generated high frequency accident condition; and
- electrical system equipment to function during normal and exceptional frequency ranges.

6.2.6. Fast transients

The design of the UK EPR electrical distribution is robust against the occurrence of identified fast transients.

6.2.6.1. Over voltage transients

The design of the EPR electrical distribution is robust when taking into account the occurrence of identified fast transients generated either by switching impulses in the network, or conducted lightning impulse after failure of the External High Voltage (EHV) lightning arrester.

From Sub-chapter 8.4, over voltages arising from switching impulses in EHV and 10 kV networks (the latter voltage affecting either the LGi or LHi systems) are protected against by surge arrestors as the first line of defence. Lightning protection is addressed in Sub-chapter 8.4 with reference to details of requirements for achieving this. Insulation coordination in the context of over voltages is also addressed within Sub-chapter 8.4.

The ability of the electrical distribution network and equipment to withstand over voltages generated by the above fast transients will be verified as follows:

- **Step 1**: identification and description of the fast transient scenarios:
  - consideration of the failure of one barrier that increases the threat on the downstream equipment;
  - definition of the network characteristics with the capacitances and impedances relevant in high frequency phenomena; and
  - establishing the criteria for assessing the risk.
- **Step 2**: investigation and choice of a transient modelling method (such as the ElectroMagnetic Transient Program software, EMTP-RV) to enable further analyses and development:
  - understanding of the phenomena;
  - analysis of results;
  - comparison with the equipment characteristics;
  - evaluation of different mitigation solutions; and
  - definition of a bounding case, if possible, to limit the scenario analyses.

The characteristics to be modified and/or the mitigation to be implemented will be included in the equipment technical specifications based on the results of the fast transient analyses.

6.2.6.2. Fast transients generated by ferro resonance

The design of the EPR plant is robust when taking into account identified fast transients generated by ferro resonance.

Ferro resonance phenomena are erratic and difficult to analyse and to reproduce. They occur on low-loaded networks with inductive and capacitive components that could resonate after an initiating event such as a circuit breaker opening. The phenomenon decreases quickly if the network is loaded.

These phenomena will be better characterised as follows:

- **Step 1**: identification of the relevant ferro resonance scenarios:
  - establish the network characteristics based on the capacitance and inductance of the equipment which are relevant to high frequency transients.
- **Step 2**: transient modelling method (such as EMTP-RV):
  - modelling and understanding of the phenomena;
  - analysis of results;
  - comparison with the equipment characteristics;

- evaluation of different mitigation solutions; and
- definition of a bounding case, if possible, to limit the scenario analyses.

The licensee will check the consistency of the design with the fast transient and ferro resonance bounding cases.

6.2.7. Harmonics

Externally generated harmonics are attenuated by the TS, TA and Power Transformer (TP). Analysis will demonstrate that adequate attenuation is achieved.

There is no physical protection from internally generated harmonics. The mitigation and management of such harmonics is addressed by a combination of designing equipment to minimise the generation of harmonics and/or to be capable of withstanding the effects of harmonics in AC and DC networks. Such design requirements will be controlled within the Books of Specific Technical Clauses (BSTCs). Analysis will demonstrate tolerability to internally generated harmonics arising from the equipment design. Coordinating the requirements in the BSTCs and the analysis will be an iterative process.

6.2.8. PSA Reliability Data

The PSA model determines the overall failure probability to supply power from at least one EDG following a LOOP.

The PSA model also provides equivalent data for supplying power from at least one UDG following a SBO, where the failure probability of the UDG could increase with the severity and complexity of the transients.

The UK EPR electrical distribution system is designed with the required level of robustness to meet the intended safety functions. If insufficient feedback experience is available for specific equipment, arrangements will be established during site licensing to demonstrate the robustness of the electrical distribution system.

6.3. SEGREGATION, ELECTRICAL ISOLATION AND SEPARATION

The mitigation of internal hazards is performed via physical separation or segregation.

All electrical safety classified equipment of the EPR plant is subject to electrical separation rules.

At the generic design stage:

- With regards to segregation:
  - Sub chapter 8.4 describes the application of RCC-E to the UK EPR project and;
  - Sub-chapter 13.2 provides an overview of the internal hazards mitigation methods. An engineering methodology and design doctrine (e.g. segregation of electrical divisions) is performed in accordance with the cabling design principles outlined in Sub-chapter 8.4.

- With regards to electrical separation:
    - Chapter D 7310 of the AFCEN RCC-E code [Ref-1] applies if the room is only concerned by electrical risk. The divisional separation is guaranteed by distancing and;
    - Chapter D 7400 of the AFCEN RCC-E code [Ref-1] requires electrical separation per electrical levels. Sub-chapter 8.4 describes the application of RCC-E to the UK EPR project.
- With regards to electrical isolation:
    - Chapter D 7500 of the AFCEN RCC-E code [Ref-1] requires electrical isolation in the same division between equipment belonging to different safety classes. For an electrical system, this is guaranteed via electrical protection selectivity and the classification of the protective device according to the highest class of the interconnected equipment.
    - Chapter D 7330 of the AFCEN RCC-E code [Ref-1] does not require separation between safety classified and non-classified cables in the same division. Sub-chapter 8.4 describes the application of RCC-E chapter D 7330 to the UK EPR project. Subsequently those cables are identified and are classified as the cables of the highest class with which they are routed;

During site licensing, measures will be taken to demonstrate that the project engineering specification will be performed in accordance with the separation rules and the cabling design principles are met.

6.4. DIVERSIFICATION IN DESIGN

6.4.1. PSA Requirements

PSA Level 1 studies specify the need for diversification associated with electrical safety classified equipment.

The equipment for which diversity is required is:

- EDGs and UDGs and;
- batteries.

6.4.2. Internal Sources EDGs and UDGs

The main Common Cause Failures between the EDGs and Ultimate Diesel Generators are analysed and identified. Mitigation of Common Cause Failures is specified in the equipment specification.

At the generic design stage:

- a definition of how diversification and redundancy are implemented during the design to ensure the independence of the EDGs and UDGs on EPR FA3 is provided [Ref-1] and;
- other regulatory requirements concerning the Ultimate Diesel Generators are defined (see Sub-chapter 9.5).

These requirements are incorporated in the technical specifications for the EDGs and UDGs.

During site licensing, proof of diversity will be provided by the licensee.

6.4.3. Batteries (Uninterruptible Power Supply)

The batteries used for the UPS are lead-acid batteries of diverse manufacture (from different suppliers and different factories) between divisions 1 and 2 and divisions 3 and 4.

At the generic design stage, information on manufacturer diversity for the mitigation of the main CCFs is required (see Sub-chapter 8.3).

During site licensing, diversity is taken into account, if required, and is confirmed by the supplier in compliance with the equipment specification.

6.4.4. Dual power sources for the control supply of switchboards

The tripping and closing supply for switchgear is provided from a supply diverse supply from the switchboard power. The control supply is established within each switchboard.

The tripping and closing supplies for circuit breakers on each safety division are sourced from the auxiliary power supply bus, which is dual supplied via power conversion modules self-contained within the switchboard.

One of the auxiliary supplies is sourced from switchboard LVi, a 400V UPS supplied switchboard. The other supply is sourced from the LAi switchboard, a 220V DC UPS supplied switchboard.

For HV switchboards, the auxiliary supply is sourced from LVi via a rectifier and diode and from LAi via a diode.

For LV switchboards, the auxiliary supply is sourced from LVi via a rectifier and diode and from LAi via a DC-DC converter and a diode.

LVi sources can be connected to the next train (train 1-2; train 3-4) in maintenance configuration only.

The two control voltages for all HV and LV circuit breakers are monitored separately.

All auxiliary supply buses on the network are dual supplied. Both supplies run concurrently and have 100% capacity. Each individual supply acts as the back-up supply in the event of failure of the other supply; a UPS supplied switchboard supplies both.

The control bus supply on switchboards LVP & LOF, LOG, LOH and LVS & LOI on divisions 1, 2, 3 and 4 respectively are all equipped with a third supply. The third supply is auto-sourced. In the event of 12-hour battery operation, the control bus supply shall be manually switched to the auto-sourced supply.

At the generic design stage:

- the single line diagram provides the power supplies to the switchboard control voltage; and
- the control voltage within the switchboard is specified in the technical specification and the implementation is based on supplier choice [Ref-1].

During site licensing:

- the licensee should verify the single line diagram complies with the diversification principle; and
- these arrangements should be confirmed by the supplier in compliance with the equipment specification.

6.5. PREVENTION OF CASCADING FAILURES BETWEEN LEVELS

With reference to the levels of defence, the design of the UK EPR electrical distribution provides electrical protection, isolation devices and diversity between the grid connection and EDGs (level 2 and 3), the EDGs and UDGs (level 3 and 4) and the UDGs and 12-hour batteries (within level 4).

- The electrical protection selectivity and isolation devices between the grid connection and EDGs are addressed in Sub-chapters 8.1 and 8.3.
- The electrical protection selectivity, isolation devices and engine diversity between the EDGs and UDGs are addressed in Sub-chapter 8.3. together with the identification of the main Common Cause Failures between the EDGs and Ultimate Diesel Generators (see Sub-chapter 8.3);
- In the event of SBO with failure of the UDGs, the 12-hour batteries supply power to the loads.

7. ROBUSTNESS AGAINST COMPONENT FAILURE

The safety equipment chosen for the UK EPR is shown to be reliable and robust in all plant conditions through good operating experience feedback.

7.1. EQUIPMENT SPECIFICATION

The equipment specification is a detailed document which is integrated in the general electrical design. The design parameters are taken into account either in the specification or in the contract technical appendices. A more detailed description of the design process is provided in section 5.2 of this sub-chapter.

The equipment specification contains generic design requirements which are:

- interface characteristics: e.g. rated voltage and power, dielectric insulation level in accordance with the design analysis (see section 6.2 of this sub-chapter);
- conditions of use: environmental conditions, expected lifetime, exceptional conditions, etc;
- performance characteristics: guaranteed or rated losses, maximum heating, etc;
- technology choice which might be specified;
- design specifications: equipment related, etc;
- manufacturing specifications: fabrication or engineering requirements, quality monitoring, etc;
- series and model test specifications; and
- supplier documents to be provided.

At the generic design stage, the equipment technical specification is provided.

During site licensing, the contract technical appendices and the technical specification targets will be provided.

7.2. FEEDBACK EXPERIENCE AND CHOICE OF EQUIPMENT

With regard to equipment robustness and reliability, equipment selection is based on operating feedback from French and international NPPs (N4 and Konvoy electrical systems plants).

Feedback experience from French, German or international plants is integrated, for each item of equipment or contract. The design feedback experience is considered when updating the equipment technical specification.

A project document provides information on the feedback to be considered in the contract technical appendices of the electrical equipment.

At the generic design stage, in order to ensure that equipment is able to operate whatever the specified ambient conditions (see Sub-chapter 8.3), a list of small electrical equipment and Instrumentation and Control (I&C) equipment with good experience feedback, or qualified equipment, is provided [Ref-1].

During site licensing, this list will be checked and updated in order to reflect UK EPR specific details. The technical specification produced for FA3 will be updated to reflect the UK EPR design.

7.3. RELIABILITY DATA

In order to ensure that safety equipment is reliable, the following features are specified, Failure Modes and Effects Analysis (FMEA), fault trees, fault on demand rates, fault in service rates and Mean Time To Repair (MTTR) as follows:

- FMEA based on IEC 60812 [Ref-1];
- fault trees based on IEC 61025 [Ref-2]; and
- fault on demand (gamma) rates, fault in service (Lambda) rates and MTTR.

At the generic design stage, these features are defined in the equipment technical specification.

During site licensing, the target values are specified in the equipment contract technical appendices. General characteristics, values of ratings, reliability and maintenance features, are provided by the suppliers in compliance with the equipment specification for each item of equipment chosen.

7.4. PECS AND SOFTWARE RELIABILITY

Smart devices in electrical equipment are used as little as possible. Their use is tracked and controlled by mean of an exhaustive list of Programmed Electrical Components (PECs) and dedicated Programmable Logic Controller (PLC) integrated into various types of safety-class F1A/B or F2 electrical and electro-mechanical equipment supplied under EPR project contracts for the Flamanville 3 (FA3) unit. Smart devices used for classified functions will be identified as soon as their suppliers are chosen. Smart devices may be required for Class 1, 2 or 3 systems, with appropriate substantiation according to the classification level (see Sub-chapter 7.7, section 3.3).

At the generic design stage, the EPR FA3 list is provided [Ref-1].

During site licensing, an equivalent list based on UK EPR equipment will be provided.

During the detailed design stage, the software of smart devices will be verified and validated as part of the I&C aspects of the design; and the functional requirements of the devices will be met in all cases.

At the generic design stage, qualification of PECs is performed according to chapter C 5333-4 of the AFCEN RCC-E code [Ref-2] and is based on current FA3 experience.

SUB-CHAPTER 8.6 – REFERENCES

External references are identified within this sub-chapter by the text [Ref-1], [Ref-2], etc at the appropriate point within the sub-chapter. These references are listed here under the heading of the section or sub-section in which they are quoted.

2. IMPLEMENTATION OF PREVENTION AND PROTECTION AGAINST COMMON CAUSE FAILURE

2.4. GENERIC ARGUMENTS

[Ref-1] Design and Construction Rules for Electrical Components of Nuclear Islands. RCC-E. AFCEN Edition. December 2005. (E)

5. HUMAN FACTORS

5.2. DESIGN, MAINTENANCE AND OPERATION

5.2.1. Documentation and Human Resources

[Ref-1] Design and Construction Rules for Electrical Components of Nuclear Islands. RCC-E. AFCEN Edition. December 2005. (E)

5.2.3. Provision of Interlocks

[Ref-1] Key interlock principles. ECEMA080959 Issue A1. EDF. August 2011. (E)

6. AVAILABILITY OF THE INTERNAL NETWORK AND ASSOCIATED EQUIPMENT

6.2. ROBUST DESIGN OF POWER SOURCES

6.2.1. Current Coordination

[Ref-1] International Standard. International Electrotechnical Commission – Short-Circuit currents in three-phase A.C System. IEC 60909-0. 2001. (E)

[Ref-2] Design and Construction Rules for Electrical Components of Nuclear Islands. RCC-E. AFCEN Edition. December 2005. (E)

[Ref-3] Detailed design for the conventional island. Calculation of three-phase short-circuit currents for the HVA and LV switchboards. ENSEMD090233 Revision A. EDF. September 2009. (E)

ENSEMD090233 Revision A is the English translation of ENSEMD070136 Revision A.

6.2.2. Protection Selectivity

[Ref-1] Design and Construction Rules for Electrical Components of Nuclear Islands. RCC-E. AFCEN Edition. December 2005. (E)

[Ref-2] Principle of selectivity and coordination of HVA and LV electrical protection systems for the EPR. ENSEMD090015 Revision A. EDF. February 2009. (E)

ENSEMD090015 Revision A is the English translation of document ENSEMD080064.

6.2.3. Voltage Coordination

[Ref-1] Design and Construction Rules for Electrical Components of Nuclear Islands. RCC-E. AFCEN Edition. December 2005. (E)

[Ref-2] Detailed design of the conventional island. Study of electrical transients. ENSEMD090232 Revision A. September 2009. (E)

[Ref-3] System Design Manual GPA: Electrical protections for the generator and transformers Part 2: System Operation. ETDOFC080364 Issue B1. EDF. January 2010. (E)

[Ref-4] System Design Manual – 10 kV Normal Power Supply System (Conventional Island) (LGi), Part 5 - Instrumentation and Control. ETDOFC070285 Revision B1. EDF. November 2009. (E)

[Ref-5] System Design Manual – 10 kV Emergency Power Supply System (LHi), Part 2 – System operation (Stage 2).
EZE/2007/en/0036 Revision D. EDF. October 2008. (E)

6.2.5. Frequency Transients circa 50Hz

[Ref-1] Design and Construction Rules for Electrical Components of Nuclear Islands. RCC-E. AFCEN Edition. December 2005. (E)

[Ref-2] System Design Manual GPA: Electrical protections for the generator and transformers Part 2: System Operation. ETDOFC080364 Issue B1. EDF. January 2010. (E)

6.3. SEGREGATION, ELECTRICAL ISOLATION AND SEPARATION

[Ref-1] Design and Construction Rules for Electrical Components of Nuclear Islands. RCC-E. AFCEN Edition. December 2005. (E)

6.4. DIVERSIFICATION IN DESIGN

6.4.2. Internal Sources EDGs and UDGs

[Ref-1] Independence of the EDG/UDG on EPR FA3 n° ECEMA091072 A. EDF. July 2009. (E)

6.4.4. Dual power sources for the control supply of switchboards

[Ref-1] UK Project - Single Line Diagram Nuclear Island-Conventional Island - FA3 pre-sizing ETDOFC/080299 Revision B. EDF. June 2009. (E)

7. ROBUSTNESS AGAINST COMPONENT FAILURE

7.2. FEEDBACK EXPERIENCE AND CHOICE OF EQUIPMENT

[Ref-1] List of the Small Electrical and Instrumentation Equipment for the EPR Plant. ECEMA040711 Revision C1. EDF. August 2010. (E)

7.3. RELIABILITY DATA

[Ref-1] International Standard. International Electrotechnical Commission – Technical Analysis for system reliability – Procedure for failure mode and effects analysis (FMEA). IEC 60812. Second Edition. 2006. (E)

[Ref-2] International Standard – International Electrotechnical Commission – Fault Tree Analysis. IEC 61025. 2006. (E)

7.4. PECS AND SOFTWARE RELIABILITY

[Ref-1] The list of programmed electrical components (PECs) and dedicated Programmable Logic Controller (PLC) integrated into various types of safety-class F1A/B or F2 electrical and electro-mechanical equipment supplied under EPR project contracts for the Flamanville 3 (FA3) unit ECEMA 070291 Revision E1. EDF. June 2010. (E)

[Ref-2] Design and Construction Rules for Electrical Components of Nuclear Islands. RCC-E. AFCEN Edition. December 2005. (E)