




<b>UK EPR</b>		
	Title: PCSR – Sub-chapter 18.1 – Human Factors	
	<b>UKEPR-0002-181 Issue 06</b>	
Total number of pages: 136		Page No.: I / VI
Chapter Pilot: A. GODY		
Name/Initials  Date 14-11-2012		
Approved for EDF by: A. MARECHAL		Approved for AREVA by: G. CRAIG
Name/Initials  Date 15-11-2012		Name/Initials  Date 15-11-2012

### REVISION HISTORY

Issue	Description	Date
00	First issue for INSA information.	18.12.07
01	Integration of technical and co-applicant review comments	28.04.08
02	PCSR June 2009 Update: <ul style="list-style-type: none"> <li>– Clarification of text</li> <li>– Inclusion of references</li> </ul>	23.06.09
03	Issue for INSA review (new section 5)	07.10.09
04	PCSR Step 4 submission: <ul style="list-style-type: none"> <li>– Sections 5 and 6 added covering normal operation procedures, operating limits, periodic tests and in-service inspection</li> <li>– Introductory text added</li> <li>– Cross-references to other PCSR sub-chapters added</li> </ul>	28-11-2009
05	Consolidated Step 4 PCSR update: <ul style="list-style-type: none"> <li>- Significant chapter update: <ul style="list-style-type: none"> <li>- Integration of human factors in design process detailed</li> <li>- Task analysis process for substantiation of human based safety claims for pre-fault and post fault actions included</li> <li>- Inclusion of misdiagnosis and violations added</li> <li>- Overall description of the approach to human factors in the EPR design restructured.</li> <li>- Summary of changes: <ul style="list-style-type: none"> <li>• Section 1 Objectives of the Human Factors Engineering (HFE) Programme replaced by Human Factors Engineering (HFE) Programme Management</li> </ul> </li> </ul> </li> </ul>	31-03-2011

Continued on next page

<b>UK EPR</b>		
	Title: PCSR – Sub-chapter 18.1 – Human Factors	
	<b>UKEPR-0002-181 Issue 06</b>	Page No.: II / VI

REVISION HISTORY (Cont'd)		
Issue	Description	Date
05 cont'd	<p>Consolidated Step 4 PCSR update (cont'd):</p> <ul style="list-style-type: none"> <li>Section 2 Human Factors Engineering (HFE) Programme replaced by Operating Experience Review</li> <li>Section 3 Design Principles for the Human-Machine Interface has been replaced by Functional Requirements Analysis and Function Allocation</li> <li>Section 4 Human Machine Interface Systems has been replaced by Human Reliability Analysis</li> <li>A new section 5 has been introduced and details the task analysis process</li> <li>A new section 6 has been introduced to cover staffing, qualifications and work organisation</li> <li>The human-machine interface (HMI) design is now presented in section 7.</li> <li>Section 8 has been introduced to detail procedure development</li> <li>A new section 9 describes training programme development</li> <li>HFE Verification and Validation is now dealt with in section 10</li> <li>Section 11 has been introduced to detail design implementation</li> <li>Section 12 has been introduced to Human Performance Monitoring</li> </ul>	
06	<p>Consolidated PCSR update:</p> <ul style="list-style-type: none"> <li>References listed under each numbered section or sub-section heading numbered [Ref-1], [Ref-2], [Ref-3], etc</li> <li>Title of Chapter 18 changed to "Human Factors and Operational aspects" and title of Sub-chapter 18.1 changed to Human Factors.</li> <li>Overall structure of Sub-chapter 18.1 has been changed from the NUREG 0711 based structure to the following overall structure: <ol style="list-style-type: none"> <li>1. Introduction</li> <li>2. Overall Basis for Safety</li> <li>3. Integration of HFE into Design</li> <li>4. Safety Arguments and Evidence</li> <li>5. Identification and Substantiation of Human Based Safety Claims</li> <li>6. HF Process Assurance</li> </ol> </li> </ul> <p style="text-align: right;">Continued on next page</p>	15-11-2012

<b>UK EPR</b>		
	Title: PCSR – Sub-chapter 18.1 – Human Factors	
	<b>UKEPR-0002-181 Issue 06</b>	Page No.: III / VI

REVISION HISTORY (Cont'd)		
Issue	Description	Date
06 cont'd	<p>Consolidated PCSR update (cont'd):</p> <ul style="list-style-type: none"> <li>- References updated to reflect latest versions of documents, and new references added as required.</li> <li>- Section 1 has been revised to summarise UK requirements for the Human Factors element of a pre-construction safety case, including discussion of ALARP.</li> <li>- Section 3 on Human Factors integration provides a summary of the process for FA3 and UK EPR specific Human Factors studies; evidence from the studies and Human Factors activities is included in sections 4 and 5 to support claims on aspects of the design and operating concepts.</li> <li>- Summaries of the results of UK EPR specific Human Factors analyses (Type A, B and C) have been added.</li> </ul>	

<b>UK EPR</b>		
	Title: PCSR – Sub-chapter 18.1 – Human Factors	
	<b>UKEPR-0002-181 Issue 06</b>	Page No.: IV / VI

**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 EPR™ 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™ 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

<b>UK EPR</b>		
	Title: PCSR – Sub-chapter 18.1 – Human Factors	
	<b>UKEPR-0002-181 Issue 06</b>	Page No.: V / VI

## TABLE OF CONTENTS

1. **SAFETY REQUIREMENTS**
  - 1.1. **REGULATORY FRAMEWORK, EXPECTATIONS AND STANDARDS**
  - 1.2. **SAFETY OBJECTIVES**
  - 1.3. **SCOPE**
  - 1.4. **INTERFACES WITH OTHER PARTS OF THE PCSR**
2. **OVERALL BASIS FOR SAFETY**
3. **INTEGRATION OF HUMAN FACTORS INTO THE DESIGN OF THE UK EPR**
  - 3.1. **FA3 INITIAL REFERENCE DESIGN**
  - 3.2. **UK EPR SPECIFIC HF INTEGRATION ACTIVITIES**
4. **SAFETY ARGUMENTS AND EVIDENCE**
  - 4.1. **FUNDAMENTAL DESIGN REQUIREMENTS**
  - 4.2. **GENERAL DESIGN AND LAYOUT**
  - 4.3. **HUMAN-MACHINE INTERFACE DESIGN**
  - 4.4. **OPERATING TEAM STAFFING CONCEPT**
  - 4.5. **UK EPR PROCEDURE CONCEPT**
5. **IDENTIFICATION AND SUBSTANTIATION OF HUMAN BASED SAFETY CLAIMS**
  - 5.1. **OVERALL RISK SIGNIFICANCE OF HUMAN BASED SAFETY CLAIMS**
  - 5.2. **OVERVIEW AND BASIS FOR APPROACH**
  - 5.3. **HUMAN BASED SAFETY CLAIMS IN THE PSA**
  - 5.4. **DETERMINISTIC SAFETY ANALYSIS**
6. **HUMAN FACTORS PROCESS ASSURANCE**
  - 6.1. **ROLES, RESPONSIBILITIES AND INTERFACES**
  - 6.2. **COMPETENCE ASSURANCE**
  - 6.3. **OVERSIGHT OF SUB-CONTRACTORS**

<b>UK EPR</b>		
	Title: PCSR – Sub-chapter 18.1 – Human Factors	
	<b>UKEPR-0002-181 Issue 06</b>	Page No.: VI / VI

**6.4. HFE PROCESSES AND DOCUMENTATION**

**6.5. DESIGN CHANGE CONTROL PROCESSES**

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 1 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

## SUB-CHAPTER 18.1 – HUMAN FACTORS

This sub-chapter describes how Human Factors (HF) principles, methods and standards are integrated into the UK EPR design and operating concepts.

### 1. SAFETY REQUIREMENTS

#### 1.1. REGULATORY FRAMEWORK, EXPECTATIONS AND STANDARDS

The following expectations and standards have been taken into account:

- Expectations of the UK regulator (the Office for Nuclear Regulation) [Ref-1] [Ref-2] [Ref-3] [Ref-4];
- Office for Nuclear Regulation (ONR) Technical Assessment Guides (TAGs);
- International standards, guidelines and technical guidelines [Ref-5] [Ref-6] [Ref-7] [Ref-8].

##### 1.1.1. Safety Assessment Principles (SAPs) and Technical Assessment Guides (TAGs)

The principles embodied in the Safety Assessment Principles (SAPs) have been taken into account in the HF approach for, and analyses performed in support of, the UK EPR design. Key SAPs relevant to the consideration of Human Factors during the UK EPR generic design phase include the Human Factors SAPs (EHF.1-10), the fundamental principle of As Low As Reasonably Practicable (ALARP) which is emphasised throughout the SAPs, nuclear safety and defence in depth (EKP.3), safety systems (ESS.3, 8, 9, 11 and 13), engineered safety features (ERL.3), maintenance, inspection and testing (EMT.1, 2, 4 to 8), layout (ELO.1, 2 and 4), safety measures to deliver the required safety functions (EKP.5) and the Fault Analysis principles (in particular FA.2, 6, 9, 13, 14 and 16) relating to consideration of operator actions and human error in the Deterministic and Probabilistic Safety Analyses.

Relevant expectations in the following TAGs have also been given due consideration:

- T/AST/051 –Guidance on the purpose, scope and content of nuclear safety cases;
- T/AST/005 – Guidance on the demonstration of ALARP;
- T/AST/058 – Human Factors Integration, specifically Appendix 1 which defines expectations for consideration of Human Factors at the Pre-Construction Safety Report (PCSR) stage;
- T/AST/063 – Human Reliability Analysis (HRA);
- T/AST/059 – Human-Machine Interface;
- T/AST/009 - Maintenance, inspection and testing of safety systems, safety related structures and components;
- T/AST/010 - Early Initiation of Safety Systems.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 2 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

### **1.1.2. International Standards, Guidelines and Technical Guidelines**

Relevant international Human Factors standards and guidelines have been applied to the design of the UK EPR, including International Standards Organisation (ISO) standards, United States Nuclear Regulatory Commission (US NRC) guidance, International Electrotechnical Commission (IEC) standards, Institute of Electrical and Electronic Engineers (IEEE) standards and Electric Power Research Institute (EPRI) guidance. French norms and EDF proprietary procedures have also been used. A full list of standards and guidelines applied is provided in [Ref-1].

The design requirements for Human Factors Engineering (HFE) and for the Human-Machine Interface (HMI) are specified in the Design & Construction Rules Applicable to Electrical Equipment (RCC-E, see Sub-chapter 3.8). Technical Guidelines for use in the design and construction of new-generation Pressurised Water Reactors (PWRs) are detailed in Sub-chapter 3.1. They include the requirement for implementation of a comprehensive HFE programme (Sub-chapter 3.1 – Table 1, section C.3).

Particular attention is paid throughout the project to the development of a robust safety culture among the personnel and subcontractor companies participating in the UK EPR project [Ref-2] to [Ref-11]. Safety culture is discussed further in Sub-chapter 21.2.

## **1.2. SAFETY OBJECTIVES**

Achieving the safety, reliability and availability objectives for the UK EPR (Sub-chapter 3.1) requires systematic consideration of the role played by human operators in running the plant. Humans play an essential role in nuclear power plant operation. They play a key role in the safe operation of the plant, particularly in managing unexpected situations, reducing the potential for plant degradation in normal operation, and in the testing and maintenance of systems. However, humans may be fallible and consequently, it is important to support both positive human contributions to overall safety and to minimise negative contributions.

Human Factors have therefore been given due consideration throughout the generic design phase of the UK EPR. This includes consideration of human actions positively contributing to plant safety, and the potential for human failure events (which encompasses both human errors and design-induced violations), and the impact of these on the plant, personnel and the environment.

The PCSR aims to demonstrate prior to commencement of construction, that sufficient analysis and engineering substantiation have been performed to give high confidence that the declared safety objectives of the UK EPR are met.

In relation to Human Factors, the overall objective is to ensure that the risk of human failure events adversely affecting nuclear safety is ALARP for the generic design of the UK EPR. The application of Human Factors approaches contributes to ALARP objectives (Sub-chapter 3.1) through the following:

- Human Factors studies of predecessor design and operating concepts to identify strengths to be retained, and evaluate options for improvements;
- the identification and analysis of Human Based Safety Claims (HBSC) and the identification/substantiation of controls to mitigate risks;
- more broadly through the integration of Human Factors principles, standards requirements and assessments to the design of the UK EPR.



<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 3 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

Human Factors also contributes to achieving the radiation protection objectives (Sub-chapter 12.0).

### 1.3. SCOPE

The level of safety demonstration that can be performed is dependent on the design development progress. The HF analyses and reviews carried out in support of the safety demonstration for the generic design, and summarised in this sub-chapter, are at the level of generic design and operating concepts rather than detailed design. This reflects the status of design development as defined in the UK EPR Reference Design Configuration for the generic design phase [Ref-1]. In accordance with [Ref-1], the HF analysis and review of high level design and operating concepts is within the scope of the safety demonstration. These include:

- computerised operation of the plant from the Main Control Room (MCR), using the Process Information and Control System (MCP [PICS]) as the preferred HMI – see section 4.3.2.1.1 of this sub-chapter;
- back-up control and monitoring provisions in the form of:
  - The Safety Information and Control System (MCS [SICS]) which provides the operators with sufficient information and controls to reach and maintain the plant at safe shutdown in the event of loss of the MCP [PICS] (see section 4.3.2.2.1 of this sub-chapter);
  - A Non-Computerised Safety System (NCSS), which provides the controls and indications to enable the operator to reach and maintain a stable state in case of total loss of computerised I&C functions (see section 4.3.2.2.2 of this sub-chapter);
- the State Oriented Approach (SOA) to incident and accident operation which is provided to support fault diagnosis and response (see section 4.5 of this sub-chapter and Sub-chapter 18.3);
- Automatic Diagnosis (AD) of the strategy to apply in the event of an emergency (see section 4.3 of this sub-chapter and Sub-chapter 18.3);
- the operating concept of an Operator Action (OA), Operator Strategy (OS) and Safety Engineer (SE) – see section 4.4.2 of this sub-chapter.

A discussion of the UK EPR design and operating concepts is provided in [Ref-2] and [Ref-3].

In accordance with [Ref-1], detailed implementation for the following items is outside the scope of the GDA safety demonstration:

- team organisation;
- staffing;
- operating and maintenance procedures;
- use of State Oriented Approach;
- display breakdown;

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 4 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

- training.

Safety culture is addressed in Sub-chapter 21.2, which describes the management system.

A summary of general design and layout for decommissioning is provided in section 4.2 of this sub-chapter. A detailed discussion of decommissioning is presented in Chapter 20. Human Factors considerations for construction and installation of equipment are summarised in section 3 of this sub-chapter. It is the responsibility of the future licensee to ensure that Human Factors issues relating to the construction, commissioning and decommissioning phases are given further consideration during the detailed design phase.

The HF studies and design support described in this sub-chapter as part of the safety demonstration are based on the information available at the time of the assessment. The UK EPR design is under development, and the HF studies are therefore based on a number of assumptions. It is the responsibility of the future licensee to verify these assumptions, and to assess the impacts of any changes to design, operating concepts and safety analyses on the HF work performed to date. Assumptions underpinning the GDA HF studies have been identified and recorded. Section 6.4.2.2 of this sub-chapter describes the GDA assumptions management process.

The HF element of the UK EPR safety case is based on the results of:

- the HFE programme for the EPR Flamanville 3 (FA3) Initial Reference Design;
- additional HF analyses and reviews to meet UK expectations and context.

### **1.3.1. Scope of the HFE programme for FA3 Initial Reference Design**

The HFE programme for the FA3 Initial Reference Design covers both the nuclear and conventional islands, including the Main Control Room (MCR), Remote Shutdown Station (RSS) and other plant locations where operations and maintenance activities take place. The HFE programme includes all plant operating categories, including normal, emergency and Severe Accident management operation (see Sub-chapters 18.2 and 18.3 for further discussion on plant operating categories).

Particular emphasis has been given to the MCR, as this is the main location for monitoring and control of the plant.

Due consideration has also been given to HF issues associated with maintenance and testing, and to other activities with high nuclear safety, personnel safety, environmental, and availability requirements, or for which certain technical changes have been envisaged. These include, for example, fuel handling, steam generator inspection, Reactor Coolant Pump maintenance, and waste processing (see section 3 of this sub-chapter for more details).

The FA3 Human Factors Engineering programme therefore applies to operational activities (including equipment isolation and testing), technical logistics (for example scaffolding) and maintenance. Testing is covered by both operational and maintenance activities.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 5 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

### 1.3.2. Scope of UK EPR specific HF activities

Some additional HF activities have been carried out in support of the safety demonstration to address differences between French and UK licensing expectations and safety case practices. Key differences include the principle of demonstration of ALARP, the claims-argument-evidence approach to safety cases, and the expectation to substantiate Human Based Safety Claims in the safety case using recognised HF methods such as task analysis. The scope of UK EPR specific HF activities includes:

- identification and analysis of pre-fault human actions during normal operation that may degrade mitigation system availability (Type A claims), or contribute to an initiating event (Type B claims). Further discussion is provided in section 5 of this sub-chapter;
- task analysis and substantiation of high and medium risk significant post-fault HBSCs (Type C claims). This includes both MCR and local-to-plant actions. Type C claims identified as low risk significant were not subjected to detailed task analysis on the basis that they do not contribute significantly to the increase in Core Damage Frequency (CDF) or Large Release Frequency (LRF). The process for sentencing and analysis of Type C claims is discussed in section 5 of this sub-chapter;
- analysis of specific HBSCs in the deterministic analyses. (Steam Generator Tube Rupture of a single tube, heterogeneous boron dilution, internal flooding and dropped loads). This is discussed further in section 5 of this sub-chapter;
- identification of 'holistic' claims on aspects of UK EPR design and operation which support human reliability, and development of supporting arguments and evidence to substantiate these. Section 2 of this sub-chapter summarises the holistic claims made in the safety case for the generic design;
- identification of inputs to the design of UK EPR specific systems. This is discussed in sections 3 and 4 of this sub-chapter.

## 1.4. INTERFACES WITH OTHER PARTS OF THE PCSR

### 1.4.1. Interfaces within Chapter 18

Sub-chapter 18.1 provides the main discussion of the HF element of the UK EPR safety case, including the overall basis for safety, the process for integrating Human Factors into the UK EPR design and safety arguments and evidence relating to both 'holistic' and specific Human Based Safety Claims. Sub-chapters 18.2 and 18.3 present additional descriptions relating to normal and abnormal operation of the UK EPR. Cross-references between the sub-chapters are provided as appropriate.

Sub-chapter 18.2, Normal Operation, outlines the methods for establishing design limits and conditions for the UK EPR. It details the arrangements to ensure that the requirements and assumptions contained in the PCSR safety demonstration are captured in operating documents. Sub-chapter 18.2 also describes the principles of normal operation, normal operating procedures, periodic testing and in service inspection.

Sub-chapter 18.3, Abnormal Operation, describes the principles, requirements and procedures for emergency operation, including use of the State Oriented Approach (SOA) and the Automatic Diagnosis (AD) system. It includes a discussion of Severe Accident management principles and procedures. It describes the UK EPR plant operating categories. Sub-chapter 18.3 also includes a discussion on emergency preparedness.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 6 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

#### **1.4.2. Interfaces with other parts of the PCSR**

Human Factors is linked to many other elements of the UK EPR safety case. References to, and interfaces with, other chapters of the PCSR are provided, where relevant. The main interfaces are summarised below:

- Sub-chapter 3.1 describes the general design and safety aspects of the UK EPR, including a summary of HF considerations applicable to the generic design phase. It provides a summary of the fundamental EPR design requirements and how these contribute to reducing sensitivity to human error.
- Sub-chapter 6.4 outlines the criterion for the habitability of the Main Control Room during accident recovery. It also defines specific MCR habitability guidelines.
- Chapter 7, Instrumentation and Control (I&C), presents the principles for, and descriptions of, the UK EPR I&C. This includes the Human-Machine Interfaces in the MCR and other plant locations. Chapter 7 includes HF related claims and cross-references to Sub-chapter 18.1 where appropriate.
- Chapter 8 presents the Electrical Systems element of the UK EPR safety case. It includes HF-related claims and cross-references to Sub-chapter 18.1 where appropriate.
- Sub-chapter 9.1 covers fuel handling and storage including operator actions associated with core loading.
- Sub-chapter 9.4 discusses environmental conditions.
- Sub-chapter 9.5 discusses UK EPR communication systems and lighting.
- Chapter 11 describes the design basis and functional requirements for the UK EPR waste treatment and storage facility. It discusses operator doses and the necessity for the production of appropriate procedures at a later phase of the UK EPR design process. The development of these procedures will require consideration of Human Factors but this aspect is outside the scope of the generic design phase.
- Sub-chapter 12.4 outlines the radiological protection guidelines, along with acceptable dose uptake levels for personnel, in relation to the ALARA (As Low As Reasonably Achievable) principle.
- Sub-chapter 13.2, Internal Hazards Protection, covers the identification and analysis of internal hazards. Analysis of Human Based Safety Claims associated with this element of the safety case is presented in section 5 of this sub-chapter.
- Chapter 14 presents the design basis analysis for the UK EPR. This analysis explicitly identifies a number of claims on operator actions. Additional implicit claims associated with nuclear risk significant plant and equipment have been identified by Human Factors studies. The substantiation of explicit and implicit design basis claims on human reliability is discussed in section 5 of this sub-chapter.
- Chapter 15 presents the objectives, scope and results of the Probabilistic Safety Analysis (PSA) conducted for the UK EPR, including the process for Human Reliability Analysis. Task analysis has been carried out to substantiate risk significant Human Based Safety Claims in the PSA. This is described in section 5 of this sub-chapter.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 7 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

- Sub-chapter 16.2, Severe Accident Analysis, addresses and defines Severe Accident scenarios. A number of Human Based Safety Claims associated with Severe Accident response have been identified during the generic design phase and assessed through task analysis. These are discussed in section 5 of this sub-chapter.
- General ALARP principles (not specific to the HFE programme) are outlined in Chapter 17. A discussion of how the HFE programme contributes to the overall ALARP objectives is provided in Sub-chapter 18.1.
- Chapter 20 identifies HF requirements for the decommissioning phase, such as ease of removal of equipment and dismantling, access requirements, personnel dose uptake and hazard identification. HF considerations relating to decommissioning are discussed in Sub-chapter 18.1.
- Chapter 21.2 describes the management system, including safety culture.

## 2. OVERALL BASIS FOR SAFETY

This section summarises the UK EPR Human Factors claims that support nuclear safety. The overall Human Factors claim is that the risks associated with nuclear safety are minimised in accordance with the ALARP principle at the GDA phase. The table below lists the key Human Factors claims which support this overall claim and form the basis of the safety demonstration for the generic design. A summary of key supporting arguments associated with each of the above groupings of claims is also provided in the table below (bulleted list following each claim). Cross-references to the sections of this sub-chapter which provide the arguments and evidence associated with each claim are provided in parentheses. The claims fall into three main groupings as follows:

- Human Factors integration into the generic design;
- UK EPR generic design and operating concepts;
- the identification and substantiation of Human Based Safety Claims that have been assessed to significantly impact on safety.

Other provisions within the generic design that support reliable human performance are also presented in this sub-chapter. Examples include features of the design which are provided to support situational awareness, communication and collaboration within the operating team. Explicit Human Factors related claims on these aspects are not made during the generic design phase, since supporting arguments and evidence cannot be sufficiently elaborated. Therefore, claims associated with these elements will need to be elaborated during the Licensing phase. Human Factors aspects that cannot be determined or resolved during the GDA phase have been identified and recorded for further consideration and resolution during the Licensing and subsequent lifecycle phases.

The claims identified in the table below, and in subsequent sections of this sub-chapter, form the basis of the HF element of the safety case for the generic design.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
		PAGE : 8 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

***Overall Claim: The risk of human failure events adversely affecting nuclear safety is ALARP for the generic design of the UK EPR.***

***Sub-claims associated with Human Factors Integration into the generic design:***

***Human Factors principles, standards, requirements and assessments have been integrated into the generic design of the UK EPR, in particular for allocation of function, the principal Human-Machine Interfaces involved in monitoring and controlling nuclear safety, the Main Control Room and the general layout of the plant for operation and maintenance (section 1.1.2 of this sub-chapter – summary of overall standards and requirements, section 3 of this sub-chapter - HF integration process, and section 6 of this sub-chapter – HF process assurance).***

- The application of Human Factors principles and standards to the generic design can be expected to promote high levels of human performance in operational tasks on a nuclear power plant.
- The EPR is an evolution of existing PWR designs; the approach for integrating Human Factors into the generic design has therefore focused on the identification of improvements to the design based on operational experience (OPEX), the identification and retention of features which support reliable human performance, and the assessment of UK EPR specific design features.
- The HFE programme for the FA3 Initial Reference Design included user requirements capture based on extensive use of OPEX to support the specification of the Human-Machine Interfaces used for controlling and monitoring nuclear safety and key operating concepts such as team organisation and the procedure concept. Human Factors specialists interpreted and implemented the captured requirements into design specifications and engineering rules. Prototypes and mock-ups of Human-Machine Interfaces used for controlling and monitoring nuclear safety were evaluated by Human Factors specialists and, together with other inputs, design specifications were adjusted and amended. Therefore, the principal Human-Machine Interfaces that can influence the performance of tasks that affect nuclear safety have been designed according to recognised Human Factors processes that will ensure generally acceptable levels of human performance.
- A four stage process of requirements capture based on OPEX feedback, specification development, modelling and prototyping, and design adjustment was undertaken for the Main Control Room of the FA3 Initial Reference Plant Design. The Main Control Room has been verified to meet the requirements of the Reference Design operating team for aspects such as space and access, visual and verbal communication, and collaborative working.
- A four stage process was also undertaken to ensure that space and layout requirements throughout the station were adequate for operation and maintenance of the Reference Design. This included HF studies of activities with potentially high nuclear safety, personnel safety, environmental and availability requirements, or for which certain technical innovations or design changes have been envisaged. The resulting specifications and recommendations resulting from the studies should ensure that the generic design provides sufficient functional space and an appropriate layout to meet operational and maintenance needs.
- Human Factors programmes are being implemented as part of UK EPR specific design changes as appropriate to ensure that the design supports reliable human

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
		PAGE : 9 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

performance.

- Human Factors aspects that cannot be determined or resolved during the GDA phase have been identified and recorded for further consideration and resolution during the detailed design phase. Assumptions have also been recorded for verification during the detailed design phase (e.g. relating to detailed Human-Machine Interface design, procedures design, team design and training).

***Sub-claims associated with UK EPR design and operating concepts:***

***The UK EPR design reduces the sensitivity of the plant to human error (section 4.1 of this sub-chapter):***

***Functions have been appropriately allocated between humans and automation and dependence on human action is minimised (section 4.1.1 of this sub-chapter).***

***Adequate grace periods are provided for in the design for the claimed operator actions (section 4.1.2 of this sub-chapter).***

- The EPR basic safety functions and detailed allocation of function between humans and automation has been derived from Konvoi and N4. The role of the operator and allocation of function is therefore based on established approaches within the EDF fleet.
- Human Factors principles and automation criteria have been developed and applied to ensure that the allocation of function to humans and automation supports reliable human and overall system performance. These are based on recognised international guidance and OPEX.
- Human Factors evaluation of allocation of function choices has been carried out as part of the FA3 HFE programme, with particular emphasis on new design features such as Automatic Diagnosis. The appropriateness of allocation of function decisions for risk significant post-fault operator actions has been assessed and substantiated to a level appropriate to the generic design phase as part of the UK EPR Type C HBSCs task analysis programme.
- Requirements for grace periods for the UK EPR are defined in the safety analysis rules, for both MCR and local-to-plant actions. The grace times are consistent with the HSE SAPs. In accordance with the ALARP principle, extended operator grace times have been achieved through the design of the protection system, larger SG inventory and pressuriser steam volume to improve management of transients.

***The general design and layout of the UK EPR support the reliable performance of operation and maintenance activities in locations closely associated with nuclear safety (section 4.2 of this sub-chapter).***

- The design and layout of the UK EPR Main Control Room, which is the central location for monitoring and control of the plant, is based on the FA3 Initial Reference Design, which is an evolution of the N4 series. It is therefore based on established principles and approaches within the EDF fleet.
- A user-centred design process, including extensive use of OPEX, was followed to define and validate requirements for design and layout of the MCR and its annexes, including working environment, layout, access and provision of equipment. This should

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 10 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

ensure that the design supports user requirements and reliable performance.

- The UK EPR MCR design incorporates a number of features to support situational awareness, effective co-ordination and communication between members of the operating team, and other teams such as maintenance. These are important considerations for reliable human performance.
- Suitable back-up and emergency management facilities are provided as part of the generic design, and these have been subject to HF input as part of the FA3 HFE programme to ensure that user requirements are supported.
- Human Factors considerations have been taken into account in the general design and layout of other UK EPR buildings and facilities where operations and maintenance activities take place. This includes consideration of working environment conditions, communications systems, workplace design and layout to reduce the potential for errors and design-induced violations during the performance of operations and maintenance tasks.

***The design of UK EPR Human-Machine Interfaces in the MCR and other plant locations, including the Remote Shutdown Station (RSS), supports reliable human performance (section 4.3 of this sub-chapter):***

***The UK EPR MCR provides the operators with all of the information, controls and means of communication they need to reliably monitor and manage the status of the power plant and its operation in all plant states (section 4.3.2 of this sub-chapter).***

***The Process Information and Control System (MCP [PICS]) provides the operators with all the information control, monitoring and information processing resources necessary to reliably operate and monitor the plant (section 4.3.2.1.1 of this sub-chapter).***

***The Safety Information and Control System (MCS [SICS]) provides the operators with sufficient information and controls to reach and maintain the plant at safe shutdown in the event of loss of the MCP [PICS]. In particular, the transfer from MCP [PICS] to MCS [SICS] and subsequent operation from the MCS [SICS] can be reliably performed (section 4.3.2.2.1 of this sub-chapter).***

***The Non-Computerised Safety System provides the controls and information to enable the operator to reach and maintain a stable state in case of total loss of computerised I&C functions (section 4.3.2.2.2 of this sub-chapter).***

- The UK EPR Human-Machine Interface design is based on the FA3 Initial Reference Design, which in turn is based on the N4 series. The HMI is therefore based on established principles and approaches within the EDF fleet. In accordance with the ALARP principle, improvements have been made to the FA3 Initial Reference Plant Design HMI design based on N4 OPEX to provide the operators with additional response time and reliable information to manage the plant and reduce the potential for human errors during plant operation.
- Human Factors studies have been carried out as part of the FA3 HFE programme to define and validate requirements for the main HMIs used to monitor and control the plant (MCP [PICS], and MCS [SICS]) and other aspects of the design important to nuclear safety such as the alarm system. The UK EPR task analyses of post-fault claims have substantiated aspects of the HMI design (controls, indications and alarms) in relation to specific operator actions, at a level appropriate to the generic design



UK EPR	PRE-CONSTRUCTION SAFETY REPORT	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 11 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

<p>phase.</p> <ul style="list-style-type: none"> <li>• A Human Factors assessment of MCP [PICS] to MCS [SICS] transfer and operation from the MCS [SICS] has also been carried out as part of the UK EPR specific HFE work programme. This concluded that the generic design and other aspects, such as the procedure and staffing concept, support reliable transfer to and subsequent operation from the MCS [SICS].</li> <li>• The HMI in the RSS is designed to enable the operators to bring the reactor to a safe shutdown state and maintain it in that state. Previous EDF plant series used conventional HMI in the RSS. The UK EPR RSS HMI design incorporates computerised MCP [PICS] workstations similar to those in the MCR including Protection System Operator Terminal (PSOT) terminals to improve functionality and consistency in operation between the MCR and RSS in relation to previous EDF plant series.</li> <li>• Human Factors principles and requirements are being incorporated into the design and assessment of UK EPR-specific HMIs important to nuclear safety, specifically the NCSS and the PSOT.</li> </ul>
<p><b><i>The operating team staffing concept applied in the generic design supports the reliable operation of the plant in all operating modes and categories (section 4.4 of this sub-chapter).</i></b></p> <ul style="list-style-type: none"> <li>• The FA3 operating team staffing concept is indicative for the UK EPR generic design. Guiding principles, based on OPEX and international guidance, have been developed and applied to the design of the FA3 operating team staffing concept. Appropriate consideration has been given to important aspects such as minimum shift complement and roles and responsibilities of the operating team.</li> <li>• Human Factors studies have been carried out to validate the operating team staffing concept applied in the generic design as part of the FA3 HFE programme, including evaluation of different MCR team organisation arrangements through simulations of emergency operating scenarios. The results of the UK EPR specific Type C task analysis programme also demonstrate that the basic operating team staffing concept applied in the generic design supports the reliable performance of post-fault actions, including prevention and recovery from potential human errors.</li> </ul>
<p><b><i>The UK EPR procedure concept applied in the generic design supports reliable human performance during activities that could impact on safety. In particular, the State Oriented Approach supports reliable fault diagnosis and response (section 4.5 of this sub-chapter).</i></b></p> <p><b><i>The risk of misdiagnosis is minimised by the State Oriented Approach, Automatic Diagnosis, operating team organisation and specific design features (section 4.5.5 of this sub-chapter).</i></b></p> <p><b><i>The risk of deliberate violation in the UK EPR by operators and maintainers is minimised by the UK EPR design and procedure concept (section 4.5.6 of this sub-chapter).</i></b></p> <ul style="list-style-type: none"> <li>• The FA3 Reference Design operating procedure concept is an evolution of the N4 and other series of French NPPs, and is therefore based on existing principles and approaches within the EDF fleet. In accordance with the ALARP principle, it incorporates features to enhance the reliability of task performance based on OPEX.</li> </ul>

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 12 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

- The SOA approach, and associated procedures used for emergency operation, is designed to provide a robust response to faults that are beyond design basis or that represent an accumulation of faults. When operating in the State Oriented Approach, required operator responses are based on the continuous monitoring of a limited set of key safety functions, regardless of the sequence of failures or events that led to the state. There is one procedure per strategy to provide the operating team with a global approach to the strategy for fault management, rather than separate procedures for primary and secondary side actions. This supports situational awareness, communication and collaboration between the various members of the operating team.
- Human Factors principles, requirements and studies have been carried out as part of the FA3 HFE programme to support the design and assessment of the State Oriented procedures, to ensure that they meet user requirements, and support reliable human performance. The results of the task analyses of Type C HBSCs provide support for the emergency operating procedure concept (i.e. SOA) and procedure design principles applied in the generic design.
- An assessment of the potential for, and defences against, misdiagnosis has been carried out as part of UK EPR specific HFE activities to demonstrate that the potential for misdiagnosis is minimised in the generic design phase. This concluded that the EPR incorporates several lines of defence to mitigate the potential for misdiagnosis and that the risks from misdiagnosis are demonstrably ALARP for the GDA phase.
- The impact of violations for the UK EPR will be significantly mitigated due to the presence of automated plant state monitoring and fault detection to allow rapid detection and recovery from induced fault states. A user-centred design approach has been followed, including extensive use of operational experience (OPEX). This has enabled previously encountered design issues that could incentivise violation to be designed out. The UK EPR task analyses of both pre- and post-fault Human Based Safety Claims included consideration of the potential for design-induced violations, and the recommendations from the task analyses will be used to support the detailed design, so as to ensure that potential violations are appropriately mitigated.

***Sub-claims associated with the identification and substantiation of Human Based Safety Claims that have been assessed to significantly impact on nuclear safety:***

***Human Based Safety Claims (i.e. claims on operator action made in probabilistic and deterministic safety analyses) have been identified and substantiated to a level appropriate to generic design assessment using recognised Human Factors methods (section 5 of this sub-chapter).***

- The process used to identify and substantiate Human Based Safety Claims for the GDA safety demonstration is based on a combination of OPEX, safety analysis and Human Factors analysis methods, such as task analysis and Human-HAZOPs. The level and scope of identification and HF substantiation performed is commensurate with the information available during the generic design phase. Collectively, the scope and level of assessment of HBSCs provides breadth of coverage in relation to the different categories of HBSCs (Type A: pre-fault human errors which degrade mitigation system availability; Type B: pre-fault human errors leading to an Initiating Event; and Type C: post-fault); types of Human failure event (human errors and violations); task types and characteristics (operations and maintenance tasks, MCR and local-to-plant locations, long and short duration tasks, different performance shaping factors); plant operating states; and operating categories (normal, emergency and Severe Accident).

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 13 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

- Particular focus has been paid to areas that it is considered will derive the most nuclear safety benefit from Human Factors assessment during the generic design phase. These include the assessment of risk significant post-fault claims on operator action, and the identification and analysis of potential human errors associated with maintenance, testing and calibration tasks for risk significant systems modelled in the PSA. Therefore, it is unlikely that human error mechanisms which could significantly affect nuclear risk have remained unidentified for analysis and assessment.
- The UK EPR specific HFE programme of work included the identification and assessment of Type A pre-fault HBSCs associated with maintenance, testing and calibration activities on risk significant equipment modelled in the PSA. Focusing on this sub-set of Type A HBSCs was judged to provide the most potential to benefit nuclear safety at the GDA stage, as it enabled the identification and assessment of risk significant Type A human failure events associated with planned maintenance on safety related equipment. Recommendations for control measures to reduce the risks associated with Type A human errors for safety significant equipment to ALARP have been identified through this process.
- Type B HBSCs have been identified through a combination of formal Human Factors analysis of generic maintenance, testing and calibration tasks associated with risk significant equipment modelled in the PSA, OPEX, and studies of specific safety case topics (e.g. dropped loads, heterogeneous boron dilution faults). These three sources provide broad coverage of potential safety significant Type B human errors or violations. An assessment of the adequacy of control measures for Type B HBSCs associated with generic maintenance, testing and calibration tasks was carried out using the approach followed for Type A HBSCs. This provided recommendations to reduce the risks to ALARP during the detailed design phase. A review has also been carried out to assess and substantiate the Type B HBSCs associated with specific events where an explicit estimation of the human error probability has been performed to derive the initiating event frequencies in the UK EPR PSA. This provided justification for the initiating event frequencies modelled in the UK EPR PSA, and evidence of the adequacy of the OPEX process used to ensure that learning is incorporated into the generic design. Based on the results of the review, it is considered that the generic design includes appropriate barriers developed through OPEX to minimise the risk associated with the Type B human failure events modelled in the UK EPR PSA.
- Human Factors analysis has been carried out to substantiate potentially risk significant Type C HBSCs (i.e. to demonstrate that required tasks are feasible and can be reliably performed). The analysis undertaken on the HBSCs has been sufficiently thorough to provide confidence that most time constrained post-fault tasks assessed for error are feasible within the time available when undertaken in the assumed task environment. The analyses generally demonstrate that the generic design incorporates Human Factors principles sufficiently to ensure the feasibility of those tasks having a risk significant relationship to nuclear safety. No fundamental issues with the UK EPR design or operating concept have been identified through the HF analysis of HBSCs, and it is therefore appropriate that options are evaluated and agreed during the detailed design phase. Where tasks have been identified to be of questionable feasibility, or where Human Factors issues remain unresolved, processes have been put in place to ensure that the issues can be understood and addressed during the detailed design phase.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 14 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

### 3. INTEGRATION OF HUMAN FACTORS INTO THE DESIGN OF THE UK EPR

*Human Factors principles, standards, requirements and assessments have been integrated into the generic design of the UK EPR, in particular for the principal Human-Machine Interfaces involved in monitoring and controlling nuclear safety, the Main Control Room and the general layout of the plant for operation and maintenance.*

The EPR is an evolution of existing PWR designs; the approach for integrating Human Factors into the design has therefore focused on the identification of improvements to design based on OPEX, the identification and retention of features which support reliable human performance, and the assessment of UK EPR specific design features. The following sections summarise the process for integrating Human Factors into the FA3 Initial Reference Design, and into UK EPR specific design activities and analyses. An overview of the Human Factors Approach used for the EPR design and compliance with international Standards is provided in [Ref-1].

#### 3.1. FA3 INITIAL REFERENCE DESIGN

Section 3 of this sub-chapter describes the Human Factors integration process only. Where HF studies or other aspects of the FA3 HFE programme provide arguments or evidence for a UK EPR design feature or operating concept, a cross-reference to section 4 (safety arguments and evidence) is provided.

This sub-section summarises the process followed to integrate Human Factors principles, requirements and approaches into the FA3 Initial Reference Design.

The process for taking account of HF in the Initial Reference Design for the FA3 plant involved a number of design studies. These started in 1986 and continued throughout the following phases:

- Preliminary studies : "Preparatory phase" (1986 - 1993) ; "Consolidation phase" (1993 - 1995) ; "Basic Design phase" (1995 - 1997) ; "Basic Design Optimisation phase" (1997 - 1998) ; "Post Basic Design Optimisation phase" (1999 - 2000);
- "Detailed Design Studies phase" (2000 onwards).

##### 3.1.1. General Methodology

These design studies took advantage of the experience acquired by EDF in the field of HFE, in particular in the design and operation of the N4 series of plant units, which was also the subject of a detailed HF approach to support the design of the HMIs in the computerised control room.

An iterative design approach including 4 main stages was developed to define and validate the HFE design choices:

- stage 1: Analysis of existing situations (previous designs, comparable existing operations, OPEX);
- stage 2: Contribution to specifications;
- stage 3: Modelling and prototyping for review of preliminary design specifications;
- stage 4: Adjustment of design specifications.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 15 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

Sub-chapter 18.1 - Figure 1 illustrates this iterative approach [Ref-1] [Ref-2]. The iterations in this figure show that the process does not stop with the analysis of user needs, but continues throughout the specification and testing period.

Application of this methodology to operation of the plant is described in section 3.1.3 and in section 3.1.4 of this sub-chapter for layout of the control rooms, general layout and maintenance.

### **3.1.2. Implementation of the Methodology for Allocation of Function**

Functional Requirements analysis and function allocation analysis have been carried out at different stages of the FA3 HFE programme, in an iterative manner [Ref-1] [Ref-2]. These studies defined and validated the principles for allocation of safety actions between humans and the systems covered by the HFE design studies.

The process followed included the following stages:

#### **3.1.2.1. Stage 1: Analysis of Existing Situations**

Based on OPEX (from the N4 plants in particular), the HF specialists prepared an initial list of operational criteria to decide which tasks should be automated.

#### **3.1.2.2. Stage 2: Contribution to Specifications**

Based on the criteria developed by the HF specialists, the designers provided preliminary recommendations on which operational actions should be automated.

#### **3.1.2.3. Stage 3: Review of Preliminary Design Specifications**

Operations teams at existing nuclear power plants reviewed the preliminary design specifications and suggested actions to be automated.

#### **3.1.2.4. Stage 4: Adjustment of Design Specifications**

The designers reviewed the operating team's proposals to determine which actions should be automated.

Studies were also carried out in order to determine the appropriate degree of automation for example for the automation of reactor protection actions, the control sequence automation, the automation of periodic tests and other test procedures. The work carried out as part of the FA3 HFE programme resulted in the development of new automation features for the FA3 Initial Reference Design to reduce reliance on operator action compared with earlier EDF NPPs. For example:

- additional signals to automatically trigger Safety Injection in shutdown states;
- automatic isolation of emergency feedwater system on high steam generator level;
- semi-automatic control of main steam relief trains and main steam bypass: after the target pressure is defined by the operator, cooldown is automatic;
- automatic implementation of set-points in stretch-out operation.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 16 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

OPEX from the N4 fleet has also led, for specific situations, to more extensive automation of EPR safety systems such as partial cooldown, radioactive Steam Generator (SG) isolation, start up and shutdown/stop sequences.

The results of the FA3 Functional Requirements Analyses are discussed further in section 4.1.1 of this sub-chapter.

### **3.1.3. Implementation of the Methodology for Operation of the Plant**

The scope of the FA3 HFE programme for operation of the plant includes the following aspects:

- HMI for MCP [PICS] and MCS [SICS];
- alarms;
- procedures / SOA and displays;
- team organisation.

#### **3.1.3.1. Stage 1: Analysis of Existing Situations**

This step is performed to ensure appropriate FA3 Reference Design choices, existing situations (previous designs, comparable existing operations) are analysed to understand the tasks allocated to plant personnel, conditions under which tasks are performed, and the strengths and weaknesses of previous designs. This process also provides a means to define the needs of the future users, i.e. to define operational or functional specifications. This is an ongoing process that monitors the state of existing plants and situations from which lessons can be learnt.

Various sources of information on existing situations have been analysed and used to inform the FA3 Initial Reference Design. These include:

- N4 Nuclear Power Plant (NPP) OPEX: This phase of collating plant based feedback took place from 1996 to December 1999. Within this time scale various discussions were held regarding specific topics relating to N4 design and operating concepts and subsequent evaluation of options. OPEX was obtained through application of systematic observations and interviews, questionnaires and observation of working practices. This data collection primarily focused on the Chooz and Civaux NPPs. Initial focus was placed on the HMI and task support (procedures, displays etc), team organisation, physical environment and training. Following this initial information gathering exercise, a series of observation phases were undertaken, each with a specific focus. All observations were carried out at the Chooz B Main Control Room. The first observation phase focused on plant overview panels, displays, operational logs and analogue recording devices. Following these observations further observations of shift teams were performed between December 1997 and March 1998. The specific focus of this set of observations was to evaluate the benefit of computerising the analogue recording devices, operational logs, and computerising normal operating procedures. The observations also studied the way in which the HMI is used by Shift Managers and management staff. The final phases of observations at Chooz B were held between October 1999 and December 1999, to observe the first unit outage. Specific focus was placed on equipment and resources available to personnel during unit outage, the benefits of computerising normal operating procedures, and team organisation.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 17 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

- Human Factors analysis of work practices performed for two reactor types in the existing EDF fleet (N4 and 1300 MWe plants): A comparative study of work practices in N4 and 1300 MWe plants was carried out to specifically examine handover between operators, unit status review at the start of a shift, start of shift readings, overall surveillance of plant activities, alarm management, monitoring of plant parameters, use of paper documents, waste management, periodic tests, supervision of maintenance work, and information sharing.
- Emergency operations drills: Tests of accident scenarios are conducted by EDF on a periodic basis using a simulator and are analysed in detail. These in-depth studies of human interaction with procedures are used to identify the strengths and weaknesses of emergency operations.
- Annual review by the training department: This provides feedback on training sessions, including the applicability and efficiency of operating procedures. The data from these reviews were taken into account in the FA3 Initial Reference Design, in particular as an input to the design of emergency procedures and to define the accident operating instructions drafting guide.
- Targeted interviews with operators and/or experts. The OPEX for the FA3 Initial Reference Design has been supplemented on a case by case basis by interviews with end users (operations and maintenance staff), in particular on the State Oriented Approach procedures.

The outputs from this process were used by the Operation Department to define the high level requirements for computerised operations. The requirements were reviewed in various French plants by user representatives.

**3.1.3.2. Stage 2: Contribution to Specifications**

Multidisciplinary Working Groups (WG), including user representatives, were created to define the specifications for plant operations. The HF contribution was assured through the permanent involvement of Suitably Qualified and Experienced Personnel (SQEP) in these working groups. The HF specialists involved had a strong knowledge of the OPEX gathered during the analysis described in section 3.1.3.1 of this sub-chapter. The main working groups created were in relation to the following topics:

- computerised operation principles;
- displays;
- emergency operations;
- normal operations;
- graphic object library (symbols).

The HF contribution during these working groups was to provide input from OPEX and international standards and to determine the most suitable compromise between technical constraints, operational requirements for computerised operation (initial requirements identified by the Operation Department) and HF requirements. The outputs of these working groups were the first issues of the engineering rules, which provide the design specifications (for example for alarm handling, displays) [Ref-1] to [Ref-7].

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 18 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

**3.1.3.3. Stage 3: Modelling and Prototyping for Review of Preliminary Design Specifications**

Preliminary specifications were developed for inclusion in mock-up exercises. HF studies were carried out using mock-ups to evaluate the design specifications and to verify the feasibility of the computerised operation principles defined by the Operation Department. Five operations teams from EDF plants were involved in this preliminary assessment phase [Ref-1] [Ref-2]. The main focus of the preliminary assessment phase was:

- display breakdown (status display, paper based procedure, Operating Instruction Sheets, and control display - see Sub-chapter 18.1 - Figure 2);
- structure and level of detail of hardcopy and computerised procedures;
- implementation and sequencing of procedures;
- synthesis information;
- Automatic Diagnosis concept;
- alarm system design;
- navigation principles.

A complementary test session was also undertaken [Ref-3]. Four teams participated in this additional testing phase, which focused on:

- display breakdown;
- display content and presentation of information;
- Automatic Diagnosis concept design;
- operating team staffing concept;
- library of graphic objects (symbols).

In 2001, the I&C HMI specifications were sent out to the suppliers of the various I&C systems so that they could begin to analyse the technical feasibility of the new generation, computerised I&C.

The review of the responses from the suppliers carried out in 2002 and 2003, contributed to the evaluation of the technical feasibility of the computerised operation principles proposed by the Operation Department.

At the end of this stage an analysis was carried out to ensure that operator tasks were fully covered by the I&C HMI specifications [Ref-4].

Evaluation of the MCS [SICS] is currently being performed as part of the FA3 programme; this is an ongoing evaluation, of which two test sessions have already been performed.



<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 19 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

#### **3.1.3.4. Stage 4: Adjustment of Design Specifications**

The results of the Human Factors assessments were reviewed to identify necessary changes to the design specifications. Proposed changes were accepted or rejected based on the various objectives to be achieved and on technical constraints.

The results of the tests were used to update the final I&C HMI specifications [Ref-1]. The results of the tests were also used to develop and update the engineering rules [Ref-2] to [Ref-5] and the general principles for the Flamanville 3 operating team organisation [Ref-6]. The operating team staffing concept is discussed in section 4.4 of this sub-chapter.

An example of the integration of the test results into the design specifications is the number of MCP [PICS] screens provided at each MCR workstation, which has been increased from 4 screens to 5 screens. This is discussed in section 4.3 of this sub-chapter.

#### **3.1.4. Implementation of the Methodology for Control Rooms, General Layout and Maintenance**

The same methodology for operation of the plant was implemented for control rooms (MCR and its annexes and the RSS), and for general layout and maintenance. This included the following four main stages:

- stage 1: Analysis of existing situations;
- stage 2: Contribution to specifications;
- stage 3: Modelling and prototyping for review of preliminary design specifications;
- stage 4: Adjustment of the design specifications.

##### **3.1.4.1. Layout of Control Rooms**

###### **3.1.4.1.1. Stage 1: Analysis of Existing Situations**

As described in [Ref-1], the design of the EPR MCR is based on a Human Factors analysis performed on a computerised control room (Chooz, N4 series NPP). N4 OPEX has been integrated into this analysis. This included a study of human-system interactions and operational needs to develop requirements for the design and layout of the MCR and its annexes [Ref-2]. The needs identified through this study cover aspects such as dimensions and layout, access, equipment to be provided, proximity to other rooms/areas, and environmental considerations (noise, temperature, lighting, etc), communication and interaction between members of the MCR team and with other teams (e.g. maintenance, emergency management).

###### **3.1.4.1.2. Stage 2: Contribution to Specifications**

The layout proposed for the MCR is based on the following (see [Ref-1] or [Ref-2] for more details):

- operational requirements; determined by the analysis of existing situations (N4 OPEX). For example the shift briefing table must provide a view of alarm displays. This requirement was not in the initial design for the N4 series MCR.
- requirements to satisfy standards: standards and generic design rules relating to layout.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 20 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

**3.1.4.1.3. Stage 3: Modelling and Prototyping for Review of Preliminary Design Specifications**

Test sessions with individuals with NPP control room experience were performed on a full scale mock up to evaluate the MCR design.

As part of the FA3 HFE programme, a validation study of the layout of the EPR MCR was carried out using a full-scale mock up [Ref-1]. The purpose was to validate the proposed MCR layout in relation to the needs and performance requirements of the operating team (see section 4.4 of this sub-chapter for a discussion of the operating team staffing concept). The study assessed the overall layout of the MCR and specific aspects such as design and sizing of control room spaces and workstations, physical access and movement, visual access and perception, communication and collaborative working.

**3.1.4.1.4. Stage 4: Adjustment of Design Specifications**

The results of the Human Factors assessments were reviewed to identify necessary changes to the design specifications. Proposed changes were accepted or rejected based on the various objectives to be achieved and on technical constraints.

**3.1.4.2. General Layout and Maintenance**

As for operational activities, an analysis of OPEX from existing plants was the first step in taking HF into account in the design of FA3 general layout and maintenance facilities and equipment.

**3.1.4.2.1. Stage 1: Analysis of Existing Situations**

OPEX from the following sources was used as an input to the design of local-to-plant maintenance activities for the FA3 Initial Reference Design:

**3.1.4.2.1.1. Analysis of N4 OPEX on Local-to-Plant Activities at Chooz**

The purpose of this study was to identify operating feedback relating to maintenance and local-to-plant operations in the N4 series. This included both positive aspects of design, any difficulties encountered by workers, and the design choices that caused these difficulties.

The study was based on interviews with about forty workers from different groups (field workers, tagging supervisors, operating technicians, preparation assistants, and external service providers). The following issues were specifically examined in this study:

- space (cramped conditions, under-sizing etc.);
- location of rooms (distance, positioning etc.);
- accessibility (rooms, equipment);
- handling and lifting operations (anchor points, lifting equipment and bridge cranes, elevators, hatches etc.);
- storage facilities;
- signposting (rooms, equipment, maintenance of labels etc.);
- working environment (heat, noise, etc.);

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 21 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

- communications (systems available, reliability etc.).

**3.1.4.2.1.2. Specific Human Factors Studies**

Specific HF studies have been carried out in support of the design of the general layout of the plant to facilitate maintenance activities and radiation protection. These include studies of activities with potentially high nuclear safety, personnel safety, environmental and availability requirements, or for which certain technical innovations or design changes have been envisaged. The process for selecting activities for specific HF studies and the disciplines involved is summarised in [Ref-1].

Several of the activities were analysed from a radiation protection point of view with Human Factors involvement. Examples include the following:

- the Effluent Treatment Building [Ref-2];
- Reactor Coolant Pump maintenance;
- lighting and power supplies;
- avoidance of errors associated with working on wrong train at power;
- fuel handling activities [Ref-3].

The following approach was used for these studies:

- Issues relating to the activities were identified based on available OPEX and on analysis of existing situations. Scenarios representative of the operations were defined.
- Future activities were identified and analysed in situ, if necessary using the 3D model of the plant, to assess their feasibility and to analyse the risks associated with human error. The analysis included the following topics:
  - operability and maintainability, including: storage; transport and handling; movement of people and equipment; working conditions, and emergency evacuation;
  - personnel safety;
  - hygiene and working conditions;
  - communications, and;
  - environmental protection.

**3.1.4.2.2. Stage 2: Contribution to Specifications**

The results from the HF studies and analyses performed in stage 1 were used as input data to define the HF requirements applicable to the construction of buildings, to the layout of equipment within them. The following topics were considered:

- the plant layout;

UK EPR	PRE-CONSTRUCTION SAFETY REPORT	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 22 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

- the various components, tools, communication systems and identification;
- the specifications for working environmental conditions that affect comfort, safety and quality of work (for example, lighting, noise, temperature, radiological conditions).

The HF requirements were integrated into the building specifications along with other specific design requirements in the form of Installation Rules datasheets (for example [Ref-1]. These are an important source of requirements for the design process. They provide comprehensive requirements relating to a wide range of Human Factors, maintenance, operational and accessibility considerations. They were reviewed and updated early on in the EPR design phase by working groups to bring them in line with current practice. The review process also took into account OPEX. The radiation protection rules (B2) specifically address maintenance optimisation from a radiation protection point of view, including consideration of OPEX.

The specification for equipment and component items is contained within a suite of documents. These documents are used to support the contract and procurement process for the supply of goods and engineering design services. Human Factors requirements are included in contract specific documents. Where necessary, particular attention has been made to certain pieces of equipment where Human Factors considerations have been reviewed in detail and used as an input to the specifications. Examples include the Reactor Coolant Pump bolt tightening machine and Fuel Building specification [Ref-2].

The technical call for bid documents for the supply of safety-related equipment (for example Containment Heat Removal System (EVU [CHRS]) pumps, Emergency Feed Water System (ASG [EFWS]) pumps, Component Cooling Water System (RRI [CCWS]) pumps, safety system gate valves) include a requirement for supplier analysis of the HF constraints linked to the equipment (working positions, accessibility of parts for example), the risks of error to be considered during maintenance on this equipment and the countermeasures for these risks.

The complete set of specifications was used as input data for detailed design and procurement processes (see section 6.4.1.3 of this sub-chapter for more details).

Radiation protection requirements were also included in order to reduce doses to ALARP during the performance of safety significant maintenance activities. The ALARP approach adopted for the design is consistent with the objectives of the Human Factors Engineering programme. This is because the design features that enhance radiation protection generally have a positive effect on operating conditions. Examples of EPR design features which minimise doses to operators are discussed in Sub-chapter 17.3.

**3.1.4.2.3. Stage 3: Modelling and Prototyping for Review of Preliminary Design Specifications**

The FA3 initial designs were reviewed through a 3D CAD model which provides a representative indication of the location of equipment, room layouts and accessibility for operations and maintenance activities. The FA3 HF specialist was involved in the review of those buildings with safety significance. For other buildings the HF review was led by building leads from civil engineering in collaboration with other disciplines including operational representatives. The reviews were carried out in accordance with a guide developed by the FA3 HF specialist to ensure that HF considerations were taken into account during the review (see section 6.4.1.4 of this sub-chapter).

**3.1.4.2.4. Stage 4: Adjustment of Design Specifications**

The results of the reviews are documented and issues and recommendations are taken into account in the detailed specifications and detailed design in an iterative manner.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 23 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

### 3.2. UK EPR SPECIFIC HF INTEGRATION ACTIVITIES

The development of the UK EPR specific HF design integration activities in support of the safety demonstration includes the following elements:

- The identification of Human Based Safety Claims and task analysis using recognised methods. This includes both pre- and post-fault claims and is discussed in section 5 of this sub-chapter. Specific aspects of the design and operating concepts that have been assessed as part of the HF assessments of pre- and post-fault HBSCs are discussed in section 4 of this sub-chapter.
- Human Factors input to design specifications and assessments associated with modifications to the FA3 Initial Reference Design to address UK expectations and context. The most significant design modifications from a Human Factors perspective are as follows:
  - Implementation of the NCSS - a defence in depth feature providing diversity and redundancy to the Protection System (PS) and SPPA-T2000 (Sub-chapter 7.7).
  - Protection System Operator Terminal - a dedicated Class 1 interface located in the MCR and the RSS to display and control Protection System permissives, resets and F1A manual actions when the plant is operated from the MCP [PICS].

Section 4 of this sub-chapter provides further details on HF input to the design of NCSS and PSOT. It is assumed that there will be HF input to, and verification and validation of, the detailed design of the above systems, and to any further modifications made in the detailed design phase to ensure conformance with HF standards and good practice. Chapter 21 and section 6 of this sub-chapter discuss the GDA design change control process.

## 4. SAFETY ARGUMENTS AND EVIDENCE

This section provides safety arguments and evidence for Human Factors claims associated with the generic design and operating concepts (see section 2 of this sub-chapter for a summary of the claims). Examples of arguments used to support the claims made include the overall basis for the UK EPR design and operating concepts presented (evolution of existing designs), incorporation of specific design features to support reliable performance, and the use of recognised HF processes and approaches such as review of OPEX, application of HF guidelines and HF studies/analyses as an input to design specification and evaluation.

Examples of evidence to support the claims made include the results of FA3 and UK EPR specific HF studies. It should be noted that the claims, arguments and evidence provided are those available for a generic design i.e. at the GDA phase. Substantiation of the UK design and operating concepts and demonstration of ALARP will continue in the detailed design phase. Nevertheless, specific considerations for the detailed design phase that have already been identified during the generic design phase are noted and included in the UK EPR GDA Human Factors Issues Register.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 24 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

## 4.1. FUNDAMENTAL DESIGN REQUIREMENTS

***The UK EPR design reduces the sensitivity of the plant to human error.***

This is achieved by:

- appropriate allocation of functions to humans or automation and minimising dependence on human actions (see section 4.1.1 of this sub-chapter);
- the provision of adequate grace periods for claimed operator actions (see section 4.1.2 of this sub-chapter);
- demonstration that safety-significant human tasks can be undertaken reliably (see section 5 of this sub-chapter).

Sub-chapter 18.2 describes the UK EPR normal operation operating principles and states. Sub-chapter 18.3 describes abnormal operation, including manual actions required in Severe Accidents. Sub-chapter 3.1 describes the process followed to define and classify EPR safety functions.

### 4.1.1. Allocation of Function

***Functions have been appropriately allocated between humans and automation and dependence on human action is minimised.***

The arrangements for allocation of safety functions between humans and automation for the generic design of the UK EPR are judged to be ALARP based on:

- the overall basis and approach (N4 series, use of OPEX, allocation of function studies) (see section 4.1.1.1 of this sub-chapter);
- the application of allocation of function principles and criteria to allocate functions to humans and automation (see section 4.1.1.2 of this sub-chapter);
- Human Factors evaluation and substantiation of allocation of function choices (see section 4.1.1.6 of this sub-chapter);
- the results of the UK EPR PSA as discussed in Chapter 15 and section 5 of this sub-chapter.

Allocation of function is an iterative process, and substantiation of allocation of function for operator actions claimed in the safety case will continue into the detailed design phase as part of the PSA (Chapter 15) and deterministic safety analysis (Chapter 14) processes.

#### 4.1.1.1. Overall Basis and Approach

The EPR basic safety functions and detailed allocation of function between humans and automation has been derived from Konvoi and N4. This provided a baseline that was developed through iteration to produce the FA3 Reference Design allocation of function [Ref-1], upon which the UK EPR is based.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 25 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

The results of the FA3 Functional Requirements Analyses are described in section 3.1.2 of this sub-chapter; these were carried out for each plant system and are presented in [Ref-2]. This includes a summary of the safety functions performed by each plant system, their functional classification and allocation of function (manual or automatic). The functional requirements described are consistent with the 2006 version of the Flamanville 3 Preliminary Safety Analysis Report (PSAR) and with the GDA Reference Design. No significant changes to the basic allocation of safety functions are anticipated.

The following sub-sections describe the automation principles and criteria developed as part of the FA3 HFE programme, the allocation of function for normal operation, fault transients and Severe Accidents. A summary of HF evaluation and substantiation of allocation of function choices is also provided.

#### **4.1.1.2. Automation Principles and Criteria**

To integrate HF into functional specifications, a number of principles relating to the role of human operators in the plant were defined as part of the FA3 HFE programme [Ref-1]. The principles are consistent with international guidance on allocation of function and cover the important considerations when making automation choices. The principles defined in [Ref-1] are as follows:

- The distribution of tasks between human operators and technical systems is defined to ensure that “the entity performing the operation” at a particular stage is clearly specified. The optimum distribution of functions between the human operator and the automatic control systems must be achieved by taking account of the capabilities of the human operator, the functions to be accomplished and their safety significance.
- Automatic control systems are allocated to repetitive tasks or those beyond the physiological, psychological or cognitive abilities of an operator (i.e. those involving very short response times or very large amounts of data). Such choices must also allow information relevant to the plant’s operation to be acquired and maintained: thus enabling the operators to carry out operational actions themselves in all situations whether normal or abnormal: i.e. the design must support a high level of situational awareness. Situational awareness is discussed further in section 4.3 of this sub-chapter).
- Tasks that require a rapid or very reliable response must necessarily be automated. They are:
  - actions required within 30 minutes after the first significant information is transmitted to the operator in the case of a fault transient (Sub-chapter 14.0);
  - actions required in the short term to prevent danger to personnel (for example, change over to iodine filtration in the event of activity detection in the nuclear auxiliary building) or irreversible degradation of equipment (for example lubrication of turbine bearings to prevent turbine degradation).

Grace periods for operator actions both from the MCR and local to plant are discussed in section 4.1.2.

- The relationship between operators and the automatic control systems enables the operators to have confidence in the automatic control systems and in the data supplied by the HMI. Without this confidence, the operators may inhibit or block the systems, and ultimately, may find themselves less well equipped to control the plant. In order to establish this confidence, operators can, at a minimum, understand the function of the automatic control systems. This means that operators can know what the automatic control systems do, avoiding a “black-box” approach. Sufficient relevant information on the behaviour of the automatic control systems is therefore fed back to the operators. Automation implementation must at all times leave the operators in charge of the plant, so that they can manage:
  - the diversity and variability of the operational situations that automatic devices cannot exhaustively cover;
  - possible failure of automatic devices, when takeover by manual control is required.
- The relationship between the human operators, the automatic control systems and the process enables the operators to remain in control of the functions for which they are responsible, by providing them with the necessary means of taking actions on the process, and when it is necessary, taking over automatic actions.
- The relationship between the operators and the process provide operators situational awareness of the current status of the process, and enable them to predict its future status. This requires relevant information about the process to be relayed to them, so they can understand the situation in real time. This understanding underpins the supervision and execution of manual actions. It implies an understanding of the process logic, rather than an exhaustive knowledge of the status of the plant and the process.

Over and above the broad principles, specific task automation criteria were developed for protective actions, automation sequences, periodic and other tests [Ref-1]. These were defined in a co-operative manner by designers and operation teams of existing nuclear power plants and are as follows:

Automation Criteria	
C1	Monotonous or repetitive tasks that, unless automated, would constitute an overload for the operators or are expected to lead to operator error through inattention and boredom.
C2	Actions on components required in very short timescales to keep the plant in operation or to manage transients which cannot be controlled by closed loop control.
C3	Changes to the set points for the control loop.
C4	Sequences that shutdown or start up large components, if no operator decision is required.
C5	Control, required in very short timescales, of systems involved in plant power output change.
C6	Operations required to change the plant state, which, if omitted, could result in complicated or time-consuming work.



## Automation Criteria

C7	Operations required to change the plant state, which, if performed manually, could extend the time to follow the load.
C8	Acquisition of parameter thresholds when the plant is changing state (e.g. from cold to hot shutdown).
C9	Operations to change the instrumentation and control parameters for stretch-out operation (beyond normal time length between refuelling outages).
C10	Operations required during start-up and shutdown transients that are straightforward in themselves, but may overload the operators if executed in parallel.
C11	Tasks which have to be performed frequently during start-up and shutdown transients.
C12	Tasks which consume a large amount of time during start-up and shutdown transients.
C13	Tasks which directly affect availability, particularly those which reduce the time taken to start-up and shut down.

**4.1.1.3. Allocation of Function for Normal Operation**

A decomposition of functions has been carried out for the FA3 Initial Reference Design [Ref-1]. This included a decomposition of operating tasks associated with each operating sequence (for example transition from cold shutdown to hot standby), and their allocation to humans or automation. The allocation is based on the criteria in [Ref-1] and summarised in section 4.1.1.2 of this sub-chapter.

**4.1.1.4. Allocation of Function for Fault Transients**

Reliance on human action to reach and maintain a safe state is minimised. As explained in Sub-chapter 14.0, a distinction is made between two phases of a transient:

- phase from initiating event to controlled state: only F1A functions are used in this phase;
- phase from controlled state to safe shutdown state: both F1A and F1B functions may be used during this phase.

The criterion to automate a F1A function is whether the action can be achieved within the grace period (see section 4.1.2 of this sub-chapter). The plant systems automatically perform all actions required in less than 30 minutes after the initiating event, to reach the controlled state. After this 30 minutes grace period, the required F1A actions can be performed either by manual actions or automatic functions. In addition, human actions are also allowed during the 30 minutes grace period for mitigation of event consequences.

In the large majority of cases, with the exception of some support systems as explained in Sub-chapter 3.2, the controlled state will be reached relying only on automatic F1A functions.

Chapter 14 describes the required F1A manual actions.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 28 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

#### **4.1.1.5. Allocation of Function for Severe Accidents**

Passive safety systems dedicated to Severe Accident scenarios, combined with manual actions from the MCR and local actions, provide the necessary mitigation path to limit discharges of radioactivity to the environment.

Actions required in Severe Accident conditions are mainly manual and sequential. The only automatic action required in short term is automatic opening of hydrogen mixing dampers located between the annulus and In-Containment Refuelling Water Storage Tank (IRWST). This action is required if an absolute pressure or differential pressure limit is reached, in order to ensure the homogenisation of the containment atmosphere [Ref-1].

#### **4.1.1.6. Human Factors Evaluation and Substantiation of Allocation of Function Choices**

The validation studies carried out under the FA3 HFE programme included aspects relating to the allocation of tasks between humans and automation. Particular consideration was given to the AD function because this is a new feature of the EPR. The methodology for these studies is detailed in section 3.1.3.3 of this sub-chapter.

The AD system provides the MCR operators with an automatic diagnosis of the strategy to apply in the event of an emergency (see section 4.3 of this sub-chapter and Sub-chapter 18.3 for a more detailed discussion). The results of the FA3 validation studies [Ref-1] provide support for this automation decision and its generic design.

The appropriateness of allocation of function decisions for risk significant post-fault operator actions has been assessed as part of the UK EPR Type C task analysis programme described in section 5 of this sub-chapter. This was based on an assessment of whether or not the task could be achieved within the available time claimed in the PSA, as well as a qualitative assessment of likely human failure events and any performance shaping factors which could be detrimental to the reliability of task performance, such as complexity.

In most cases, the analysis demonstrated that the required actions can be completed in the available time, and that a margin exists between the assessed and claimed task duration. Where margin exists, this provides the opportunity for detection and recovery from the potential human failure events identified through the analysis within the available time. Most of the claimed actions are MCR based, and the analyses confirmed that adequate task support (controls and displays, procedures) is provided to the operator, assuming that the detailed design issues identified through the analyses are addressed. In a small number of cases, recommendations were made for further evaluation of allocation of function for specific actions. The issues relate to detailed allocation of function considerations for specific actions rather than the basic allocation of safety functions between humans and automation. These issues are recorded in the UK EPR GDA Human Factors Issues Register (HFIR) and will be addressed during the detailed design phase.

#### **4.1.2. Grace Periods**

***Adequate grace periods are provided for in the design for the claimed operator actions.***

The grace period corresponds to the time granted to the operator from the first significant accident information until the first necessary manual action as required in the framework of the deterministic safety demonstration.

Requirements for grace periods for the UK EPR are defined in the safety analysis rules specified in Sub-chapter 14.0, Sub-chapter 3.1 – Table 1 (A2.1 and A2.3) and [Ref-1].

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 29 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

The following operator grace periods apply to the deterministic safety analyses;

- for a manual action from the MCR, no action is required until 30 minutes after the first significant information is transmitted to the operator;
- for a local manual action, i.e. a manual action that must be performed on-site, outside the control rooms, no action is required until 1 hour after the first significant information is transmitted to the operator;
- it should be noted however, that operators are allowed to take action before the specified grace time to optimise plant response. The grace periods are intended to reduce stress on the operator by providing a time margin before a manual action is required.

The UK EPR operator grace periods defined above are consistent with the HSE Safety Assessment Principles [Ref-2]. They also represent an improvement over the N4 series, which has periods of 20 minutes for operator actions in the Main Control Room and 25 to 35 minutes for those actions which are performed locally. Extended grace times for the UK EPR have been achieved through the design of the protection system, larger SG inventory and pressuriser steam volume to improve management of transients. Sub-chapter 1.3 provides a comparison of UK EPR, Konvoi and N4 systems and parameters.

Regarding operator actions claimed in the Probabilistic Safety Analysis, time available for operator action has been defined depending on the scenario. In the context of the PSA, time available for operator action is defined as the time window from the start of the event until required mitigation actions claimed in the PSA have been performed. For each operator action identified in the PSA, the available time for response is determined based on representative calculations (typically thermal-hydraulic). These define the time available to perform the claimed actions, and are based on conservative assumptions. A single calculation using a bounding scenario may be used for a similar operator action that occurs in various scenarios.

Task analysis of risk significant operator actions identified in the PSA has been carried out, including an assessment of achievability of the claimed action (i.e. whether the action can be completed within the response times defined in the PSA). If the same operator action is claimed in scenarios with different times available for operator action, then these are modelled as separate claims within the PSA. The approach and results are discussed in section 5 of this sub-chapter.

## **4.2. GENERAL DESIGN AND LAYOUT**

***The general design and layout of the UK EPR supports the reliable performance of operation and maintenance activities in locations closely associated with nuclear safety.***

This section describes the design and layout of the main EPR rooms, buildings and facilities in including arguments and evidence relating to how it supports reliable human performance. It covers the following facilities and aspects;

- Main Control Room (section 4.2.1 of this sub-chapter);
- Remote Shutdown Station (section 4.2.2 of this sub-chapter);
- Emergency Management Facilities (section 4.2.3 of this sub-chapter);
- Other Buildings and Facilities (section 4.2.4 of this sub-chapter);

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 30 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

- Design and Layout for Decommissioning (section 4.2.5 of this sub-chapter).

The scope for the generic design phase covers general design and layout only (dimensions and layout, access, equipment to be provided, proximity to other rooms/areas, and environmental considerations). The design will be developed during the detailed design phase and will comply with relevant Human Factors principles and requirements.

Human-Machine Interface design is discussed in section 4.3 of this sub-chapter.

#### **4.2.1. Main Control Room**

##### **4.2.1.1. General Requirements and Approach**

The design and layout of the UK EPR Main Control Room is based on the FA3 Initial Reference Design, which is an evolution of the N4 series. Although the UK EPR design incorporates some changes (for example, a NCSS and PSOT) the MCR retains the principal features of the FA3 Initial Reference Design.

Specifications for the layout, equipment and environmental conditions for the Main Control Room, and its annexes, are provided in [Ref-1]. As discussed in section 3 of this sub-chapter, a user-centred design process was followed to define and validate requirements for the FA3 Initial Reference Design. This included a study of human-system interactions and operational needs to develop requirements for the design and layout of the MCR and its annexes [Ref-2].

The results of this study, together with requirements derived from standards relating to the design of the Main Control Room [Ref-3], formed the basis for the MCR design and layout for the FA3 Initial Reference Design.

The FA3 validation study described in section 3.1.4.1.3 of this sub-chapter confirmed the adequacy of the general layout and features and identified recommendations for consideration during the detailed design phase [Ref-4]. For example, the OA and OS workstations were moved closer together to support communication and co-operation between the operators.

##### **4.2.1.2. General Design and Layout of the MCR**

A description and projected layout of the MCR is presented in [Ref-1]. Sub-chapter 18.1 - Figure 3 presents an indicative MCR layout drawing. The MCR includes 3 main operating work areas:

- the main operator work area (including the MCP [PICS], PSOT, Inter-Panel Signalisation Panel (PSIS), Inter-workstation console (PIPO), and Plant Overview Panel (POP);
- the MCS [SICS] work area, which includes the NCSS and a Severe Accident Panel;
- a briefing area located between the MCP [PICS] and MCS [SICS] work areas.

In addition to the main work areas defined above, other equipment is provided in the MCR. These include;

- a fire detection panel;
- a communications console for internal and external communications;
- a work area for consulting documents;

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 31 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

#### **4.2.1.2.1. Main Operator Work Area**

There are four full MCP [PICS] workstations in the MCR. Each workstation has five screens, plus an additional sixth screen, which is not connected to the process and is used for administrative functions.

Two of the four full MCP [PICS] workstations are operator workstations; one for the Operator Action (OA) and the other for the Operator Strategy (OS). These are arranged side by side.

The Shift Manager workstation is identical to the operator workstations, with access to the same MCP [PICS] displays. This workstation is planned to be used in supervision mode when used by Shift Manager (SM), and can also be used in control mode as a back-up for the other workstations.

The fourth full MCP [PICS] workstation is a 'spare' and is not permanently occupied by a member of the MCR operating team.

A separate Minimal Operator Workstation (MOW) with four screens is available to others working in the MCR to access process information without interfering with the operators at their workstations.

There are four PSOTs in the MCR; one located at each main MCP [PICS] workstation. The PSOT is dedicated to PS operation and provides Class 1 information and controls for use while operating the plant via MCP [PICS].

The number of MCP [PICS], including PSOT workstations required for the main (or 'preferred') HMI to be considered available is 1 in normal operation, 2 in emergency operation. The basis for this is as follows:

- in normal operation, the Operator Action and Operator Strategy can reorganise their workload on a single MCP [PICS] workstation and the Shift Manager does not require continuous access to a MCP [PICS] workstation.
- in emergency operation the two operators require two MCP [PICS] workstations to be available in control mode to perform their duties and the Shift Manager requires access to a MCP [PICS] workstation in supervision mode. This can be performed either on a full MCP [PICS] workstation, the MOW workstation, or the POP. The Safety Engineer uses the MCS [SICS] to perform their assigned emergency role.

A PSIS is located in front of the operators, between the POP screens. This is a conventional panel which presents information on the status of the MCP [PICS] and main I&C systems to allow the operator to assess the possible need to transfer command to the MCS [SICS].

A PIPO is located in the console between the OA and OS workstations. The PIPO is a small conventional panel which provides, amongst others, controls to manually trip the reactor, prior to evacuation, if the MCR is rendered uninhabitable (for example, due to fire).

A POP is provided at the front of the MCR.

A discussion of the MCP [PICS], PSOT, PSIS and POP HMI is provided in section 4.3 of this sub-chapter; see section 4.2.1.3.1 for a discussion of how the layout supports Situational Awareness.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
		PAGE : 32 / 130
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	Document ID.No. UKEPR-0002-181 Issue 06

#### **4.2.1.2.2. The MCS [SICS] Work Area**

The MCS [SICS] is located at the rear of the MCR. The MCS [SICS] is a conventional panel, designed for standing operation.

The MCS [SICS] is used by the whole MCR team as the operating interface when the MCP [PICS] is unavailable. A discussion of the MCS [SICS] HMI is provided in section 4.3.2 of this sub-chapter. This includes details on the Human Factors assessment carried out as part of the safety demonstration of MCP [PICS] to MCS [SICS] transfer and emergency operation using the MCS [SICS] panel.

The MCS [SICS] controls will only be enabled by the operating team if the MCP [PICS] is unavailable due to maintenance or failure. During normal operation, supervision will be performed using the MCP [PICS] on the Shift Manager workstation.

During emergency operation with the MCP [PICS] available, the Safety Engineer (SE) (or SM if the SE is not immediately available in the MCR) uses the MCS [SICS] to perform a separate analysis of the situation which is contrasted with the team diagnosis, and to verify the results of the team's activity. This provides an additional mechanism to prevent and recover from potential human failure events. The location of the MCS [SICS], separate from the computerised workstations but with visual and verbal access to the team is designed to support the role of the SE in emergency operation.

A Severe Accident management panel is provided as part of the MCS [SICS] panel. This is located in a clearly demarcated area on the left hand side of the MCS [SICS] panel and is discussed in section 4.3 of this sub-chapter.

#### **4.2.1.2.3. The Briefing Area**

A briefing area is provided in the MCR, which includes a table for use during team briefings (see section 4.2.1.3 of this sub-chapter for more details).

### **4.2.1.3. Specific Design Considerations for the MCR**

#### **4.2.1.3.1. Situational Awareness**

Situational awareness is 'the perception of environmental elements within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future'. [Ref-1] It involves being aware of what is happening in the environment in order to understand how information, events, and actions will impact goals and objectives, both current and in the near future. Situational awareness is of particular importance for the MCR operating team because the MCR is the central location for monitoring and control of the plant. An accurate global view of plant status and activities is therefore essential.

The UK EPR MCR design incorporates a number of features to support situational awareness. These include a computerised POP. The POP provides the functionality to present overview information on key plant parameters. The specific information presented on the POP is to be determined by the future licensee during the detailed design phase. More details on the POP are provided in section 4.3.2 of this sub-chapter.

The operators and Shift Manager have a direct view of the POP from their operating positions. Operation Department requirements for the POP are summarised in [Ref-2]. These include the requirement for the Shift Manager to be able to view the POP easily at all times, to support their role of 'globalising' information during normal and emergency operation.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 33 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

Improvements have been made to the EPR design to enhance situational awareness, considering N4 series experience. These include:

- MCP [PICS] overview screens at each operator workstation to provide a direct means to view the status of key plant parameters - section 4.3.2 of this sub-chapter provides more details;
- changes to the location of the table in the briefing area (see section 4.2.1.2.3 of this sub-chapter) compared to the N4 layout to enable the operating team to view alarms and the POP during shift handover. The new location supports continuous monitoring of the plant and discussion of alarms during shift handover, and a shared understanding of plant status between the incoming and outgoing team [Ref-2].

#### **4.2.1.3.2. Communication and Collaborative Working**

The physical design of the MCR incorporates a number of features to support the sharing of information, and to enhance group and individual situational awareness.

During normal and emergency operation the arrangement of the MCR workstations is designed to support effective co-ordination and communication between the OA and OS. In addition, during emergency operation, the OS checks the strategy to be applied, monitors implementation of the strategy and actions performed by the OA, and makes requests to the OA for action where necessary. The proximity of the OA/OS workstations and the provision of duplicate MCP [PICS] screens at the OS workstation support the role of the OS in emergency operation.

The Shift Manager workstation is located behind the OA and OS workstations. This enables the Shift Manager to visually supervise OA and OS actions and interaction with the MCP [PICS] system in use in order to maintain oversight of MCR operations.

The physical location of the MCR in relation to other operational facilities is designed to support frequent formal and informal interactions between members of the MCR team and with other teams such as maintenance. The Shift Manager office, I&C Maintenance Room, Auxiliary Monitoring Systems Room (which contains monitoring equipment used for periodic testing), and the Permit room (used for administrative activities associated with equipment consignment) are all located on the same level as the MCR to facilitate such interactions.

The operational needs identified in [Ref-1] (see section 3 of this sub-chapter) take account of Main Control Room staffing for the full range of operating conditions, including normal and emergency operation, start up and outages. Requirements for communication systems (for example, telephone, loudspeaker and paging systems) in the MCR and its annexes (including the RSS, Technical Support Centre (TSC), Permit Room, I&C and auxiliary monitoring rooms) are defined in [Ref-2]. Human Factors analysis of activities and N4 OPEX provided an input to the specifications [Ref-1]. Communication systems are discussed in Sub-chapter 9.5, including the site and local plant alarm systems, paging and internal and external telephone communication systems.

#### **4.2.1.3.3. MCR Working Environment**

Requirements for environmental conditions in the MCR have been studied and defined [Ref-1] [Ref-2], as part of the FA3 HFE programme. This included analysis of activities and N4 OPEX [Ref-3], see section 3 of this sub-chapter. Environmental conditions in the MCR and its annexes (for example, the RSS, TSC, Permit Room, I&C and auxiliary monitoring rooms) are discussed in Sub-chapter 9.4. Lighting is discussed in Sub-chapter 9.5.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 34 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

## Lighting

The requirements for lighting in the MCR and its annexes have been defined based on the tasks to be carried out and relevant standards [Ref-2]. The lighting in the MCR is designed to provide optimal working conditions for the operation team. This includes the provision of lighting levels suitable for operational tasks (good contrast so that the information required may be read easily), and minimising glare and reflections.

Each area within the MCR will have lighting appropriate to its particular function. This lighting will be adjustable, so the operators have adequate lighting for their tasks.

The emergency lighting in the MCR, the RSS and the TSC is supplied by four electrical divisions and backed-up by the main diesel generators (EDG). Part of this emergency lighting is also backed-up by ultimate diesel generators and emergency uninterruptible power supply (accumulator batteries) which guarantees a minimum lighting level in case of Station Black-Out (SBO).

## Acoustic Environment

Requirements relating to noise levels in the MCR and its annexes are defined in [Ref-2]. The acoustic environment and the noise levels in the MCR are specified so that the process monitoring and control and associated activities may be carried out in comfort, efficient communication is ensured between members of the operations team, and auditory signals are heard clearly. This requires a sufficiently low average background sound level, good reverberation properties in the MCR, and appropriate sound level for auditory signals.

The following measures are used to significantly reduce the noise in the MCR:

- monitoring the design and implementation of equipment that is a structural noise source and choosing its location;
- improving the acoustic isolation to reduce air-borne sound from the ventilation in the MCR, and;
- building the MCR on the “box within a box” principle.

The “box within a box” principle involves creating a closed space isolated from the main civil-engineering structure by intermediate elastic supports that dampen the vibrations transmitted by neighbouring installations.

## Thermal Environment

Optimal thermal environments can reduce the potential for fatigue, help to maintain concentration levels and reduce physical and mental stress. Human reliability may be negatively affected if the thermal environment is not optimal.

Temperature ranges for the MCR and other plant areas are discussed in Sub-chapter 9.4 and [Ref-1]. Sub-chapter 9.4 also provides information relating to the design of the air conditioning systems for the MCR.



<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
		PAGE : 35 / 130
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	Document ID.No. UKEPR-0002-181 Issue 06

#### **4.2.2. Remote Shutdown Station**

A RSS is provided to support centralised control and monitoring of the plant in the event of the Main Control Room becoming uninhabitable due to an internal hazard (for example, fire). A discussion of the RSS HMI is provided in section 4.3 of this sub-chapter. Sub-chapter 6.4 defines MCR habitability guidelines.

The RSS is located on the level below the MCR, in a different fire zone. Sub-chapter 13.2 includes a discussion how the design supports nuclear safety in relation to fire protection. As stated in Sub-chapter 7.2, the design concept is that such internal hazards in the MCR (such as fire), will not occur at the same time as other independent failures, accidents or hazards, with the sole exception of possible loss of the external power supply. Design measures have been taken to minimise Main Control Room fire hazards and provide appropriate fire detection mechanisms [Ref-1] and Sub-chapter 13.2. The constant presence of personnel in the MCR and the availability of fast and efficient fire fighting resources also contribute to reducing the risk of fire propagation in the MCR.

The RSS area is a temporary work area, which is smaller than that area occupied by the MCP [PICS] workstations in the MCR. It is normally operated by three people in the event of the MCR being uninhabitable (the OA, OS and SM) [Ref-1]. The required operator actions to transfer from the MCR to the RSS in the event of the MCR being uninhabitable are discussed in section 4.3 of this sub-chapter. Access routes are provided to enable the MCR team to reach the RSS within 30 minutes of evacuating the MCR [Ref-2].

Operational requirements for the general design and layout of the RSS have been defined and assessed as part of the FA3 HFE programme (see section 3 of this sub-chapter). This included a study of activities to be performed in the RSS at an N4 plant to identify strengths to be retained and improvements to design [Ref-3]. The requirements defined include the dimensions, access requirements, layout of the room, and equipment facilities. Details on the proposed dimensions of the RSS are defined in [Ref-1].

The RSS has two full MCP [PICS] operator workstations, and one additional Minimal Operator Workstation. These three operator workstations are installed in the same area. The RSS also has two PSOTs. No POP is provided in the RSS.

#### **4.2.3. Emergency Management Facilities**

The UK EPR design includes a TSC which provides the information and means of communication to assist with emergency operational management during accident situation by an expert support team advising the operating personnel.

Operational requirements for the TSC have been assessed as part of the FA3 HFE programme (see section 3 of this sub-chapter) and are defined in [Ref-1]. These incorporate operational needs identified through HF assessment, such as location in relation to the MCR, dimensions and layout, equipment and facilities [Ref-2].

The TSC is located near the main entrance to the control area, separate from the MCR. This location supports easy access to the TSC by personnel from different departments who may need to participate in emergency operational management. This provides a dedicated facility away from the MCR to support effective analysis and decision-making. There will be suitable provisions for effective communication between the emergency management facilities and the MCR, although the detail of this has yet to be fully defined.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
		PAGE : 36 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

## CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS

The TSC is designed to accommodate six people in an emergency situation. It has a workstation identical to the Shift Manager workstation in the MCR. All the information held in the MCP [PICS] is also available on the screens in the TSC. The TSC design also includes cabinets to house all the documentation required for emergency response, communications equipment, a meeting table and printing equipment.

Other emergency management facilities, including an Emergency Control Centre used by the Emergency Controller and their team, are also provided. Sub-chapter 18.3 provides a detailed discussion on emergency preparedness arrangements and facilities.

### 4.2.4. Other UK EPR Buildings and Facilities

Human Factors considerations have been taken into account in the general design and layout of other UK EPR buildings and facilities where operations and maintenance activities take place. This includes consideration of working environment conditions, communications systems, workplace design and layout to reduce the potential for errors and design-induced violations during the performance of operations and maintenance activities. The design of UK EPR buildings and facilities is based on the N4 series. OPEX has been incorporated into the generic design to support operability and maintainability, as part of the overall design process, and through specific HFE studies. The process for integrating HFE into the design of UK EPR buildings and facilities, including use of OPEX, is summarised in section 3 of this sub-chapter. The results of specific studies are summarised in this sub-section to provide evidence that HF has been taken into account. The process for selecting activities and disciplines involved is described in [Ref-1].

#### 4.2.4.1. Working Environment

Requirements relating to the working environment conditions for EPR buildings have been defined based on International and French standards [Ref-1], OPEX review and Human Factors studies [Ref-2]. Specific requirements are included in the building specification documents [Ref-3] to [Ref-7]. Key requirements are summarised below. Requirements for the MCR working environment are discussed in section 4.2.1.3.3 of this sub-chapter.

Thermal environment requirements for the RSS, offices, TSC and electrical rooms have been defined with regards to ambient temperature, air speed and humidity to ensure a comfortable working environment [Ref-1]. A thermostat will be located within these rooms so that the thermal environment is adjustable to suit the needs of the operator. Specific requirements have also been defined for the MCR, and are discussed in section 4.2.1.3.3 of this sub-chapter. Sub-chapter 9.4 provides a more detailed discussion on heating systems.

Design requirements for lighting have been specified [Ref-1]. These include the requirements for lighting to be designed to meet task requirements for the various working areas and adjustability of lighting levels. Lighting levels for work areas will be within the 250 and 500 lux range and 50 lux for circulation spaces. Lighting will be adequately positioned so that there are no shadow areas in the maintenance room or corridors. Wall and floor coatings will allow for good lighting of rooms and support optimal working conditions, including the avoidance of glare. Emergency lighting will be provided from an independent supply that can last for one hour at half power [Ref-1].

Noise limits are specified in [Ref-1] so as to limit operator exposure to the negative effects of high sound levels. Specific noise limits have been defined for the TSC, Permit room, RSS, I&C maintenance rooms and auxiliary monitoring rooms [Ref-1]. The selection of equipment within local-to-plant rooms will also consider potential noise sources. Selection of equipment will aim to reduce sound output where possible.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 37 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

#### **4.2.4.2. Communications Systems**

The UK EPR communications equipment and systems are based on OPEX, in particular from the N4 series. The systems include site and local alarms, a paging system and telephone systems (main and secondary). These are discussed in Sub-chapter 9.5.

#### **4.2.4.3. Local-to-Plant Activities and Layout**

A study of local-to-plant activities at the Chooz plant (N4 series) was carried out as part of the FA3 HFE programme (see section 3 of this sub-chapter for more details). As noted in section 3 of this sub-chapter, Human Factors studies have also been carried out for particular local-to-plant and maintenance activities and issues [Ref-1] to [Ref-8]. The 3D CAD model (see section 3 of this sub-chapter) has been used for specific design studies for example, for the Steam Generator bunkers and the refuelling cavity area [Ref-9] [Ref-10].

The proposed changes to the activities described above have contributed to improving the quality of the intervention by maintenance and operations personnel, and to reducing the potential for human error. Examples of recommendations to support the maintainability of the plant that have been incorporated into the UK EPR design include;

- the possibility of replacing rather than repairing equipment in order to reduce maintenance times and human error potential associated with invasive maintenance;
- the development of plans for electrical interconnections between the four trains. This is to allow power to be supplied (when needed) to those systems which must continue to function during shutdown (such as elevators and lighting). This avoids the need for temporary connections and associated potential for human error;
- the equipment (safeguard systems and their support systems) is divided between four independent divisions with independent access routes to:
  - allow maintenance to take place during plant operation; thus, maintenance operations may be spread over the entire cycle;
  - help reduce the potential for confusion between rooms and equipment.
- a room for the operating technicians has been created in the controlled area (in the Access Tower). This facilitates both the preparatory work for activities in the nuclear auxiliaries building, and co-operation and communication with the Main Control Room;
- assisted testing devices will be installed in the electrical cubicles that supply the safety valves;
- the opening diameters for access to the EPR steam generator secondary and primary sides have been increased in comparison with previous SG designs to facilitate access for staff and inspection equipment (this design aspect is discussed in Sub chapter 18.2).

The KKK system was specifically designed and introduced to the EPR in order to reduce the potential for errors linked to working on the incorrect train when carrying out at-power maintenance. This system controls access to the Safeguard Auxiliary Buildings. Human Factors specialists provided input to the design specification for this system.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
		PAGE : 38 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

## CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS

As part of the EPR approach to dose optimisation, studies of certain activities were undertaken to optimise worker doses [Ref-1] and [Ref-11] to [Ref-17]. This approach is an example of targeting of analysis effort in a proportionate manner in accordance with the principle of minimising doses to ALARA (see Sub-chapter 12.4).

In addition, the FA3 Initial Reference Design HFE programme included input to the design of local control stations that are provided in the following locations: operating water treatment plant, diesel generator buildings, waste management (filter change stations), fuel handling, polar crane, and refuelling machine [Ref-18] to [Ref-21].

### 4.2.4.4. UK EPR specific HF analyses

Potential human failure events associated with maintenance and testing of UK EPR systems and equipment (Type A and B human failure events) have been identified and assessed as part of the UK EPR specific HF activities. This included review of design and other controls to support the prevention, detection and recovery from the identified human failure events. The results are summarised in section 5.3 and 5.4 of this sub-chapter.

Design requirements and considerations identified through the UK EPR specific HF studies of maintenance and testing activities discussed in section 5.3 of this sub-chapter provide an input to design documentation and requirements for suppliers.

### 4.2.4.5. Integration of the results into the Design

Specifications have been produced for EPR buildings including the nuclear auxiliary building, safeguard auxiliary and electrical buildings, reactor building, diesel buildings and fuel building [Ref-1] to [Ref-5]. The specifications include general HF considerations and specific design requirements for construction, operation and maintenance. They incorporate requirements from applicable standards, OPEX and the results of the FA3 studies described in section 3 of this sub-chapter. The specifications are produced in accordance with guidance documents to provide a consistent approach [Ref-6]. There is also a specific guidance document on consideration of Human Factors [Ref-7].

### 4.2.5. Design and Layout for Decommissioning

The role of the operator during decommissioning is dependent on a number of factors including the phase of decommissioning (for example during defuelling and initial clean out the role typically involves surveillance, waste handling, and decontamination activities), and the decommissioning strategy adopted. The nuclear safety risk and the complexity of the plant will progressively decrease as decommissioning proceeds.

Decommissioning requirements have been taken into account in the EPR generic design. Sub-chapter 20.2 provides a base strategy plan for decommissioning and discusses design features which support access/dose reduction/ease of decommissioning.

Further assessment of decommissioning tasks and HF requirements should be carried out by the future licensee as part of development of detailed decommissioning planning activities.

## 4.3. HUMAN-MACHINE INTERFACE DESIGN

***The design of UK EPR Human-Machine Interfaces in the MCR and other plant locations, including the Remote Shutdown Station (RSS), supports reliable human performance.***

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
		PAGE : 39 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

## CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS

As stated in section 1.3 of this sub-chapter and [Ref-1], the safety demonstration for the generic design phase is limited to HMI design principles and concepts, such as the organisation and composition of computerised displays and conventional panels, alarm philosophy and generic design. The HMI design will be developed during the detailed design phase.

This section summarises the overall basis, principles and requirements for the UK EPR HMI design, and discusses how the design of the HMI in the MCR, the RSS and TSC, local control stations and local-to-plant controls supports reliable human performance.

### 4.3.1. Overall Basis, Principles and Requirements

The UK EPR Human-Machine Interface design is based on the FA3 Initial Reference Design, which in turn is based on the N4 series. The design may be adapted in the detailed design phase according to the specific British socio-cultural context, regulatory and future licensee expectations.

The design concept and principles for the HMI are similar to those applied to existing N4 French Nuclear Power Plants, including:

- a computerised HMI (mainly composed of the MCP [PICS]) to support the operating team during normal and emergency conditions;
- a back-up conventional panel MCS [SICS] to provide, the necessary controls and displays:
  - in the event of loss of the MCP [PICS]:
    - to stabilise the plant for a limited amount of time (indicative: 8 hours), then to reach and maintain the plant at safe shutdown;
    - if combined with emergency conditions, to support the operations team applying Emergency Operating Procedures;
    - to operate the plant during planned maintenance of the MCP [PICS] when the reactor is in state F.
  - in emergency operation without loss of the MCP [PICS]:
    - to support the Safety Engineer's independent permanent monitoring.

The UK EPR also includes a Non-Computerised Safety System (NCSS) and its corresponding HMI to be used in case of total loss of computerised I&C platforms.

As stated in Sub-chapter 3.1, improvements have been made to the FA3 Reference Plant Human-Machine Interface design based on N4 OPEX to provide the operators with additional response time and reliable information to manage the plant and reduce the potential for human errors during plant operation. These include;

- an AD function to reduce the potential for misdiagnosis. The AD supports the overall State Oriented Approach which aims to simplify diagnosis of, and response to faults. The UK EPR HMI is designed to support the State Oriented Approach response to faults. The AD system and State Oriented Approach is discussed further in section 4.5 of this sub-chapter and in Sub-chapter 18.3;

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
		PAGE : 40 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

## CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS

- large computerised screens (POP) to support team situational awareness (see section 4.3.2.1.4 of this sub-chapter);
- the design of MCP [PICS] overview displays to improve the operator's view of plant status and support high levels of situational awareness (see section 4.3.2.1.1.2 of this sub-chapter);
- computer based procedures for certain aspects of operation (see section 4.3.2.1.1.2 and section 4.5 of this sub-chapter);
- improved system maintainability due to the ability to separately maintain the different types of displays (status, control and instruction).

The principles of standardisation and consistency have been applied to the design of the UK EPR Human-Machine Interfaces. A minimum number of interface types have been used in the MCR (except where required for diversity reasons). Computerised workstations provided in the RSS are of the same design as those in the MCR.

To address UK regulatory expectations, the UK EPR also includes a NCSS and its corresponding HMI to be used in case of total loss of computerised I&C platforms.

The safety requirements for the MCR, the RSS and the TSC are defined in international standards [Ref-1] [Ref-2] [Ref-3] [Ref-4], French nuclear codes and standards, including the RCC-E standards, and in specific EDF standards (see Sub-chapter 3.8). The RCC-E standards cover aspects such as the way in which safety information shall be presented, features of the architecture, information and control systems (e.g. controls, coding, alarms, procedures), and control and monitoring devices used in the computerised and conventional workstations.

### 4.3.2. HMI in the Main Control Room

***The UK EPR MCR provides the operators with all of the information, controls and means of communication they need to reliably monitor and manage the status of the power plant and its operation in all plant states.***

The plant is managed and monitored in all situations from the MCR, assuming it is available. Plant management includes commissioning, maintenance, scheduled outages, operation at full power and during accidents. Early stage commissioning when the MCR is not available may need to be controlled through specific commissioning test arrangements. In addition, the MCR has facilities for internal and external communication.

The MCR is designed to remain available if there is an earthquake; thus it includes sufficient equipment provisions to ensure safe operation during and after an earthquake. Other equipment may be non-operational, but must not prevent the MCR being used, nor jeopardise systems or equipment with a safety function (Sub-chapter 7.2).

As stated in section 4.2 of this sub-chapter, if the MCR is rendered uninhabitable (e.g. due to fire), the operating team transfer to the RSS. The HMI in the RSS enables the operators to bring the reactor to a safe shutdown state and maintain it in that state (see section 4.3.4.1.1 of this sub-chapter).

The Main (or 'preferred') Operating HMIs used in the MCR are:

- the MCP [PICS] (Process Information and Control System) – for further details on the design of the MCP [PICS], refer to Sub-chapter 7.5 and section 4.3.2.1.1 of this sub-chapter;

UK EPR	PRE-CONSTRUCTION SAFETY REPORT	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 41 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

- the PSOT – see Sub-chapter 7.2 and section 4.3.2.1.2 of this sub-chapter;
- the Inter Workstation Console – see Sub-chapter 7.2 and section 4.3.2.1.3 of this sub-chapter;
- the POP – refer to Sub-chapter 7.2 and section 4.3.2.1.4 of this sub-chapter;
- the Inter-Panel Signalisation Panel – see Sub-chapter 7.2 and section 4.3.2.1.5 of this sub-chapter.

The following back-up control system HMIs are provided in the MCR;

- the MCS [SICS] (Safety Information and Control System), which includes a SA panel - for further details on the requirements of the MCS [SICS] and SA panel, refer to Sub-chapter 7.3 and section 4.3.2.2.1 of this sub-chapter;
- A conventional hardwired panel for NCSS operation – see Sub-chapter 7.4 and section 4.3.2.2.2 of this sub-chapter.

#### 4.3.2.1. Main Operating HMIs

##### 4.3.2.1.1. MCP [PICS] Workstations

***The MCP [PICS] provides the operators with all the information control, monitoring and information processing resources necessary to reliably operate and monitor the plant.***

It is the main operating interface and, when available, is used by the operators in all plant states and categories. This includes normal operation (Plant Condition Category, PCC-1) plant condition categories, PCC-2 to PCC-4 and also in Risk Reduction Categories RRC-A and RRC-B [Ref-1].

##### 4.3.2.1.1.1. Human Factors input to the design and evaluation of the MCP [PICS]

An analysis of normal, emergency and Severe Accident MCR tasks has been carried out based on the existing EDF fleet and specific features of the EPR series, which identified the needs of the operators [Ref-1]. An assessment has also been carried out to verify that the HMI principles and specifications support the tasks performed by the operating team [Ref-2].

As noted in section 3 of this sub-chapter, a HF study of normal and emergency operating scenarios was carried out using a HMI mock up as part of the process of iterative HF validation of, and user input to, the design [Ref-3]. This confirmed that the HMI principles and basic requirements for the MCP [PICS] support normal and emergency operation and no significant issues were identified. Recommendations were made for consideration as part of the ongoing design process.

A supplementary test campaign was carried out in 2005, focusing on the principles of emergency operation and other aspects of the HMI that were not sufficiently developed during the preceding tests (e.g. Automatic Diagnosis, status display, distribution of information between methods and instruction sheets) [Ref-4]. The tests resulted in recommendations on how operational requirements should be satisfied, provided an input to the development of emergency operating rules, and to the specification of the operating displays. The principles and requirements for the design and layout of the MCP [PICS] displays are described in [Ref-5].

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 42 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

The activities summarised above included the consideration and evaluation of HMI design options in relation to a number of factors including human error potential, contributing to the objective of reducing the risks from human error to ALARP.

In accordance with UK and international good practice, a style guide should be developed during the detailed design phase for the design of the MCP [PICS] and other safety related HMIs. This should ensure that the detailed design meets HF standards, UK conventions and practices. The use of a style guide will also support the goal of consistency in the design of different HMIs.

The UK EPR task analyses of Type C HBSCs included assessment of relevant aspects of the MCP [PICS] HMI design in relation to the achievability and reliability of specific claims. Aspects assessed included the cues and indications provided to the operator, navigation, and information presentation. The analyses also included the identification and assessment of potential human failure events that could result in nuclear safety-related consequences. In the majority of cases, the analyses demonstrate that the generic design of the HMI supports the achievability of required actions in the time available, and the claimed level of human reliability. Where appropriate, recommendations for consideration during detailed design have been provided to reduce the potential for human failure events, and hence contribute to the achievement of ALARP.

These are recorded in the UK EPR GDA Human Factors Issues Register. They relate to detailed design considerations such as:

- ensuring that the cues for specific operator actions associated with certain claims are clear and compelling (for example for total loss of 10KV supplies, ASG [EFWS] tank level indication, and the cue to start feed and bleed);
- consistency of information display and clarity of icons;
- provision of trend information on specific displays.

**4.3.2.1.1.2. Organisation and composition of the MCP [PICS] displays**

The MCP [PICS] displays are organised to provide a complete awareness of the status of the plant and the process before decisions are taken or actions are initiated.

The detailed structure and design of the displays will be developed during the detailed design phase; however it is envisaged to be largely based on the FA3 design.

A study of EPR operator tasks has been carried out to define the tasks performed, and identify task support requirements (display, control, feedback, communication, etc) [Ref-1]. The results of the study have been used to verify that all tasks have been taken into account in the HMI requirements and specifications [Ref-2].

A notable change from the N4 series design is the overall display composition of the MCP [PICS]. For the UK EPR, each of the four full MCP [PICS] workstations has five standardised screens. There are no dedicated alarm screens, compared to the N4 series design, which has three operations screens and four screens dedicated to the permanent display of lists of alarms. The UK EPR has a permanent header which is used to alert the operator to alarms rather than dedicated alarm screens. The provision of five standardised screens is based on: three screens for operation (one for status display, one for instruction display, one for control display) and two additional screens to provide the flexibility to display information relevant to the operator's task (e.g. to monitor specific parameters such as tank level, or to display alarm lists) [Ref-3].



<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 43 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

The display structure outlined above has the advantage of not monopolising screens to display the list of alarms when it is not necessary [Ref-4]. Since the MCP [PICS] screens are not dedicated to any particular display, the design enables the future licensee to organise the MCP [PICS] displays to meet their specific requirements. Section 4.3.3 of this sub-chapter provides further discussion of alarm system design.

Both the operator's task and the plant's operational regime (normal or emergency) determine how the MCP [PICS] displays are organised [Ref-3]. As a general rule, the set of displays is designed to minimise the number of displays used during a task. There are two main categories of display: process displays and instruction displays.

The process displays include active or interactive graphical "objects" that either provide information on the status of the process (sensors, graphs, status of components, synthesis information) or enable commands to be issued (to components, options, adjustments to settings, etc.). They also provide a means of navigating between displays. Depending on the nature of their function, they can display the status of the system or components, and, when required, send commands to change the status (start / stop, align).

The instruction displays are intended to support the operators, and display operating instructions and alarm sheets via static text.

The separation of process and instruction displays is based on review of N4 OPEX and operational requirements.

### **Process Displays**

Process displays include control displays and status displays. The availability of these two types of displays permits two complementary modes of representation of the status of the plant as follows:

- **Control displays**

These are the main displays used by operators to control and monitor plant systems. They are structured according to plant systems. The overall display format is a process schematic with interactive graphical objects allowing individual and group control of components.

The basic structure and content of the control displays is based on the N4 series design. The main changes implemented in the EPR are the ability to adjust the limits of the control displays with respect to the operation activities they display and the ability to combine displays. From a Human Factors perspective, the ability to combine displays helps operators to assimilate information and to focus on a limited number of displays, enhancing recall and reducing cognitive workload [Ref-4].

As for the N4 series, there is no need to navigate hierarchically through intermediate displays to access a display containing the required controls or information.

- **Status displays**

A status display is defined as any display which presents information but does not provide control capability. Status displays provide a higher level of abstraction and set out the overall plant functioning. There are two main types of status display; those linked to an operating strategy (normal or emergency), and other status displays to support specific activities or tasks.

UK EPR	PRE-CONSTRUCTION SAFETY REPORT	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 44 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

Status displays linked to an operating strategy display the trends and information on parameters most relevant to the operating objectives and activities in progress. They comprise embedded graphs, time-line flow diagrams and synthesis information on the systems in use, so an operator has the information that is required to gain an overall (global) view of the plant and to monitor process changes. For emergency (State Oriented) operation, there are dedicated status displays for each strategy which have a standardised layout.

Other displays to support operational management are provided to supply information about the process. These include:

- overview displays, which provide general information about the plant and its parameters. They are used to obtain quick status reports on the state of the plant during a shift or during shift change;
- displays breaking down information on synthesis displays: these are available for all the information syntheses shown on the screen and assist the operator in interpreting them;
- displays used to monitor some of the automatic sequences: these are available to allow operators to verify the proper progress of a complex automatic sequence of actions;
- displays specific to the synoptic (POP): these provide a general view of the plant, customised according to its state;
- displays used to give an Automatic Diagnosis on the status of the plant: these are specially designed to help operators to identify incident or accident states of the plant, and to propose a specific procedure to be followed according to this diagnosis. There is also a display which presents the logic for the AD diagnosis (see section 4.5 of this sub-chapter and Sub-chapter 18.3 for discussion of Automatic Diagnosis);
- displays for major components (e.g. Reactor Coolant Pump, turbine, transformer). These have been retained as a strength from the N4 series design;
- displays presenting Technical Data Sheets: these are linked to components and are composed of:
  - dynamic displays, which indicate the current status of an actuator, and;
  - static data sheets, with various information about the actuator (e.g. mechanical characteristics, geographic location in the plant).
- displays useful to members of the operating team other than operators (e.g. by the Shift Manager): these displays consolidate the information needed to assess the conditions of the plant;
- graphical trend displays of parameters selected by the operator;
- logs recording operational actions and events for use by the operating team.

The design can accommodate future licensee requirements for specific status displays to support operational management.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 45 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

## Instruction displays

The instruction displays include:

- Operating Instruction Sheets: these describe the detailed actions to take (checking and controlling components, checking parameters), and the action sequence. The Operating Instruction sheets are discussed further in section 4.5.1 of this sub-chapter on the UK EPR procedure concept;
- Alarm Sheets: alarm sheets are described in section 4.3.3.7 of this sub-chapter.

Section 4.5 of this sub-chapter provides a discussion on the UK EPR procedure concept, including both computerised and paper based procedures.

### 4.3.2.1.1.3. *Level of guidance*

The information presented via the MCP [PICS] is used during all normal operations, emergency conditions, Severe Accident management situations. The information:

- enables the priority, the severity and the impact on safety and availability of an event to be assessed, in the context of the plant's general state;
- supplies the operational procedures to guide the operator in changing the programmed status of the plant (normal operating procedures);
- supplies the operational procedures to be used during an accident;
- provides information that steers the operator towards a procedure or an alarm sheet. For instance:
  - for alarms, activating an indicator in the screen header gives access to the list of alarms, from which by clicking on one of them appears a window showing the alarm sheet with the steps to take;
  - for operational management during an accident, a dedicated indication of AD activation appears in the screen header and gives access to a status diagnosis screen. A synthesis of the results of the automated diagnosis appears in the AD overview format. From here, the operator can call up the status display associated with the strategy to be followed, and then the associated control displays.

The level of guidance provided to the operators (procedures, alarms sheets) is integrated into the computerised HMI. The information provided corresponds as closely as possible to that needed by the operator at a given moment. The use of synthesis information, and voted information to avoid indications from redundant sensors, is based on a similar principle. The level of guidance is consistent regardless of the operational procedure (normal operation, incident or accident). The instrumentation and control system does not manage the operational instructions issued by the operating team. Ensuring that the operating procedure and the operational method are followed is the sole responsibility of the operating team.

For conventional and hardwired control panels, the required documentation is available in paper format.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 46 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

**4.3.2.1.1.4. Input Devices and Navigation**

Various options for navigation to and between displays are provided. Navigation to the required display can be performed via lists of displays. The operator can also navigate between displays through active links (e.g. an arrow or graphical object). These can be accessed using a mouse. This type of navigation avoids the requirement to type characters on the keyboard to call up a display (with the associated loss of time and risk of error). It also avoids the requirement for the operator to systematically call up lists of displays to select the one of interest [Ref-1].

Operators can also access the information or controls from a system menu or by searching the code of a specific item of equipment using the keyboard.

**4.3.2.1.1.5. Control of access to MCP [PICS] functions**

Access to some operations, including controlling components individually and resetting alarms, may be restricted by administration settings at the workstation (password). A particular workstation may be designated either in control mode or supervision mode. Only authorised personnel may change this assignment (by specific password).

**4.3.2.1.2. Protection System Operator Terminal**

The PSOT is a Class 1 interface located in the MCR and the RSS dedicated to Protection System controls when operating from the MCP [PICS]. The PSOT scope includes PS permissives, resets, and manual F1A action (as defined in Sub-chapter 3.1 – Table 1, section B.2.1), as well as required information when the plant is operated from the MCP [PICS]. The PSOT is a UK EPR specific system which has been incorporated into the design to meet UK context and requirements.

The PSOT is a computer-based touch-screen unit located at each of the main 4 MCP [PICS] workstations of the MCR, and each of the 2 workstations in the RSS.

The Basis of Safety Case for the PSOT is presented in [Ref-1]. This includes preliminary requirements for the Human-Machine Interface. The PSOT will be designed in accordance with Human Factors principles, following a specific programme consistent with the overall HFE programme for the detailed design phase. This will include analysis of operator tasks, definition of HF requirements for the PSOT, and HF verification and validation of the design and operation of the system. Aspects considered will include the HMI and layout (including both hardware and software), integration into the UK EPR MCR, and task support such as operating procedures.

Sub-chapter 7.2 includes a description of the PSOT I&C.

**4.3.2.1.3. The Inter Workstation Console (PIPO)**

The Inter Workstation Console is a small conventional panel which is located between the two front operator workstations in the MCR. The PIPO includes pushbuttons to enable the operator to initiate a reactor and turbine trip, independently of the computerised HMI.

The PIPO is always active, and provides control facilities to manually trip the reactor, perform general secondary trip (including turbine trip), and open the main breakers on GEA (Turbine Group auxiliary transformer) and GEV (turbine group power transmission system). These manual commands are used during the evacuation of the MCR to the RSS.

The PIPO is a Class 1 interface. Sub-chapter 7.2 describes the PIPO I&C.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
		PAGE : 47 / 130
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	Document ID.No. UKEPR-0002-181 Issue 06

#### **4.3.2.1.4. Plant Overview Panel (POP)**

A POP incorporating large screens is installed in the MCR which is provided to promote group discussions, situational awareness and decision making. The POP can provide an overview of key plant parameters, which are presented on four large format images projected onto screens at the front of the MCR.

The provision of the POP addresses the limitations of display screens, which provide a partial view of plant status, and an individual rather than shared reference of the status of the plant [Ref-1].

The POP is designed as an aid to normal and emergency operations. The POP displays can be modified according to the status of the plant to display only relevant information to the team. The design can accommodate specific display requirements of a future licensee, including permanent overview displays.

The POP projects displays from the MCP [PICS] (retro- or video-projection) and is therefore unavailable in the event of loss of MCP [PICS]. The POP is used during all plant states to present the overall status of the plant (temperature, power ratings, etc) and its main components (e.g. reactor coolant pumps, pressuriser, SG, main valves). Information is displayed either as graphs or instantaneous values.

Requirements for the POP are specified in [Ref-2]. The POP displays will be visible and readable from the two operator MCR workstations. Human Factors studies of the POP have been carried out as part of the FA3 HFE programme including feedback from the N4 series, which substantiated the design principles and requirements for the generic design [Ref-3] and [Ref-4]. The design of the POP displays and operating principles will be finalised and validated in the detailed design phase.

Sub-chapter 7.2 provides a summary of the POP I&C.

#### **4.3.2.1.5. Inter-Panel Signalisation Panel (PSIS)**

The PSIS is a conventional panel located in front of the two front operator workstations of the MCR, between the POP screens. The location is designed to enable the operator to easily view the PSIS displays when using the MCP [PICS] in the MCR.

It presents information on the status of MCP [PICS] and the main I&C systems to allow the operator to assess the possible need to transfer command to the MCS [SICS]. It includes the following displays (no controls are provided on the PSIS);

- MCP [PICS] life-sign – this displays the status of the MCP [PICS] operator workstations – see section 4.3.2.2.1 of this sub-chapter on MCP [PICS] to MCS [SICS] transfer;
- status of the Protection System (PS);
- status of the Safety Automation System (SAS).

The PSIS includes an indication for status of the MCP [PICS] to MCS [SICS] transfer selection switches [Ref-1].

A description of the PSIS I&C is provided in Sub-chapter 7.2.

UK EPR	PRE-CONSTRUCTION SAFETY REPORT	SUB-CHAPTER: 18.1
		PAGE : 48 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS

#### 4.3.2.2. Back-up Control System HMIs

##### 4.3.2.2.1. MCS [SICS] Panel

***The MCS [SICS] provides the operators with sufficient information and controls to reach and maintain the plant at safe shutdown in the event of loss of the MCP [PICS]. In particular, the transfer from MCP [PICS] to MCS [SICS] and subsequent operation from the MCS [SICS] can be reliably performed.***

Sub-chapter 7.3 provides a discussion of the MCS [SICS] I&C, and Sub-chapter 7.5 describes modes of operation, including loss of MCP [PICS].

The MCS [SICS] is a large conventional panel located at the rear of the MCR in the emergency control area [Ref-1] with indications, recorder and controls. There are three main sections; a top section with alarms, middle level with instrumentation, and lower level with controls and instrumentation to provide feedback on operator actions [Ref-2].

The MCS [SICS] panel layout is organised according to the fundamental safety functions (reactor cooling, control of reactivity and containment).

When the MCP [PICS] is unavailable, the MCS [SICS] HMI enables the operating team to carry out the following functions [Ref-3]:

- monitor and manage the plant in a stable power state if the MCP [PICS] is not available for a limited short period under normal conditions;
- reach and maintain the plant in a safe state, if the MCP [PICS] is unavailable for a longer period under normal conditions;
- monitor and implement appropriate operational management functions following accidents, so that the plant is brought to and maintained in a safe state (respectively final, and fallback) when the MCP [PICS] is not available in a situation defined as PCC-2 to PCC-4 (RRC-A and RRC-B respectively), and;
- carry out fire-fighting actions in the nuclear island.

If the minimum requirement for operational workstations is not met, as defined in the written procedures, the operator must transfer command to the MCS [SICS] via the transfer control system. To facilitate the decision making process of transferring control to the MCS [SICS], the status of the MCP [PICS] is monitored and displayed by a Class 2 active life-sign check that indicates the status of each MCP [PICS] operator workstation on a specific indicator at the PSIS panel. When the PSIS alarm is present the operator applies a procedure for transfer.

During emergency operation, when the MCP [PICS] is available, the MCS [SICS] panel is used for the Safety Engineer role to monitor the status of the plant using the Safety Engineer procedure (state-oriented constant monitoring). It is also used by the operator and/or maintainer for periodic cross-comparison between MCP [PICS] and MCS [SICS] as part of the regular MCP [PICS] validation checks. When the MCP [PICS] is operational, the MCS [SICS] controls are disabled but the indicators and alarms are active (alarms are automatically acknowledged and silenced to avoid distracting the operators).

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 49 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

Design requirements and operating principles for the MCS [SICS] have been defined as part of the FA3 Reference Design [Ref-3] and [Ref-4]. To the extent possible, consistency has been maintained between the MCP [PICS] and MCS [SICS] HMI design (for example, coding and labelling) and operating concept (for example, the same procedure structure and contents presentation). Operation from both interfaces under emergency conditions uses the same State Oriented Approach operating procedure structure (see section 4.5 of this sub-chapter) to support reliable transition from MCP [PICS] to MCS [SICS] and for subsequent operation using the MCS [SICS] [Ref-5].

The HF studies for the FA3 Initial Reference Design described in section 3 of this sub-chapter contributed to the definition of the requirements for the MCS [SICS] (for example, coding, arrangement, and layout). An initial full-scale mock-up was produced, on which the various devices were represented. The evaluation carried out covered the MCS [SICS] structuring principles, the layout of the control, measurement and alarm zones, the hardware for the controls, measurement and alarm systems, the symbols used, the documentation, team work whilst operating at the MCS [SICS], and the communication systems.

**MCP [PICS] to MCS [SICS] Transfer and Operation from MCS [SICS]**

A Human Factors assessment of MCP [PICS] to MCS [SICS] transfer and operation from the MCS [SICS] has also been carried out as part of the UK EPR specific HFE work programme [Ref-2]. The scope included substantiation of the generic design and operating concept in relation to transfer from MCP [PICS] to MCS [SICS], and use of the MCS [SICS] to control the plant from all relevant initial plant states (normal, emergency and Severe Accident).

The assessment concluded that the MCP [PICS] to MCS [SICS] transfer strategy is based on clear and unambiguous criteria, supported by clear and unambiguous signals that the Operating Team will use to base their diagnosis on and make the decision to transfer to the SICS. It also concluded that the transfer is guided by appropriate procedural support. The operating team organisation allows for recovery mechanisms, based on the SOA, to be in place in order to capture any errors made during the transfer process and operations at the MCS [SICS].

Task analyses of two HBSCs from the UK EPR PSA have been carried out to assess transfer to, and operation from the MCS [SICS], using the Type C task analysis methodology described in section 5 of this sub-chapter. The analysis focused on detection and diagnosis of MCP [PICS] failure and diagnosis that transfer to MCS [SICS] is required, and operation from the MCS [SICS]. The analysis provides further evidence that transfer to, and operations at the MCS [SICS] supports safe operation and is ALARP at the current stage of design. Further assessment is required during the detailed design phase to fully substantiate the claims relating to MCP [PICS] to MCS [SICS] transfer and operation, based on the detailed design and procedures.

**Severe Accident Panel**

The MCS [SICS] also includes a Severe Accident Panel which is provided as an integral part of the MCS [SICS] panel, in a demarcated area. The SA panel includes the indications, alarms and controls necessary, in case of total loss of electrical power (loss of voltage on LH and LJ busbars), to identify the need to enter Severe Accident operation dedicated to this situation, and to implement the Severe Accident guidelines discussed in section 4.5 of this sub-chapter. The design of SA panel HMI will be finalised during the detailed design phase.

During SA operation, the OA and OS operate from the MCP [PICS] and the SE from the MCS [SICS]. The SA Panel includes the indications and alarms for core outlet temperature and containment dose rate, and controls for pressuriser discharge systems valves, to complement other information and controls provided for SA operation on other SICS panels.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
		PAGE : 50 / 130
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	Document ID.No. UKEPR-0002-181 Issue 06

The tasks associated with Severe Accident operation were considered as part of the task analysis of operating activities conducted as part of the FA3 HFE programme. This included the identification of design and operational requirements for the generic design [Ref-6]. This study provided an input to the requirements and specifications for the HMI [Ref-7].

Human Based Safety Claims associated with Severe Accident operation have been assessed as part of the UK EPR Type C task analysis programme, which is discussed in section 5 of this sub-chapter. The analyses [Ref-8] concluded that the claimed actions are achievable in the time available. The task analyses identified a number of recommendations to enhance the reliability of task performance, and hence contribute to minimising the risks associated with human failure events in accordance with the ALARP principle. These relate to detailed design considerations and are recorded in the UK EPR GDA Human Factors Issues Register.

#### **4.3.2.2.2. Non-Computerised Safety System (NCSS)**

***The Non-Computerised Safety System (NCSS) provides the controls and information to enable the operator to reach and maintain a stable state in case of total loss of computerised I&C functions.***

The NCSS is a UK EPR specific system that has been introduced to meet the overall I&C reliability targets.

The NCSS is designed with the capability to allow operators to manage plant stabilisation, feed and bleed operation and Severe Accident scenarios as reflected in the claims related to NCSS operation.

The Basis of Safety Case for the NCSS is presented in [Ref-1]. Functional and safety requirements for the NCSS have been defined, including preliminary requirements for the Human-Machine Interface [Ref-2] [Ref-3]. The NCSS HMI should be provided as part of the MCS [SICS] to support user requirements, and avoid constraints related to a dedicated HMI (e.g. space) [Ref-1].

Claims made on operator action using the NCSS have been assessed and substantiated to a level appropriate for the generic design phase, through the UK EPR Type C task analyses discussed in section 5 of this sub-chapter and reported in [Ref-4]. The HF analysis performed to substantiate specific claims on operator actions has also identified HF design requirements for the NCSS, which are recorded in the UK EPR GDA Human Factors Issues Register.

Detailed requirements for the NCSS HMI, including grouping and demarcation of controls and information, will be defined and evaluated in the detailed design phase.

### **4.3.3. Alarms**

#### **4.3.3.1. Principles and Requirements**

An alarm is an alert message delivered by the instrumentation and control system to the operators warning them of an anomaly in the plant's operation or status. It requests them to take the appropriate action to manage the situation [Ref-1].

The main media for presentation and response to alarms is the MCP [PICS]. As stated in section 4.3.2.2.1 of this sub-chapter, when the MCP [PICS] is operational, MCS [SICS] alarms are active but alarms are automatically acknowledged and silenced to avoid distracting the operators. In the event that the MCP [PICS] is unavailable due to maintenance or failure, alarms display and response is provided via the MCS [SICS].



<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 51 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

The alarm system is designed to support the reliable detection, diagnosis and response to anomalies in the plant's operation or status. The principles for specifying and handling alarms are based on the N4 series and lessons learned through OPEX [Ref-2]. These include classification of alarms based on severity only, rather than both severity and urgency (see discussion below), providing alarms that are easily interpretable by the operator to facilitate diagnosis, and distinguishing alarms from equipment faults to avoid distracting the operator from functional alarms requiring operator action.

Requirements for alarm system design have been developed and assessed as part of the FA3 HFE programme [Ref-3] [Ref-4]. Detailed principles and specifications on the design of alarms have also been developed for system engineers [Ref-5] [Ref-1]. These are based on the principles and requirements defined through OPEX and formal HF studies.

Alarm flooding can overload the operator, increasing the potential for human errors during detection and response to alarms. The UK EPR design includes features to reduce the potential for alarm flooding. These are discussed in [Ref-1] and include;

- filtering by conditioning alarms based on plant state. This reduces the number of active alarms displayed to the operator; only those relevant to the current state are displayed;
- filtering of redundant or lower priority alarms;
- automatic clearing of alarms when parameters return to normal or are no longer applicable due to changes in plant condition.

#### **4.3.3.2. Alarm Classification**

Each alarm has a classification that determines how it is displayed on the operational interfaces (colour, flashing light, audible signal). This makes it easier for the operators to decide on priority when they have multiple alarms to manage.

Severity is the only criterion used to classify alarms. This design decision is in response to N4 Operation Department feedback requests to simplify the classification criteria, due to the potential confusion generated by using a second criterion (urgency). Urgency would have to be considered in relation to a number of factors including the degree of automation, the presence of limitations, and the protection of equipment [Ref-1].

If a function or a system malfunctions, the severity of an alarm depends on its impact on the plant's operational management at the time it appears.

Four levels of severity are defined in the FA3 Reference Design. The classification is in increasing order of severity. The levels are listed below:

##### **Severity-1 alarm**

These alarms indicate either occurrence of a minor fault, possibly the precursors of the future loss of a significant equipment item (1st-stage fault), or that the system is approaching a threshold that will initiate automatic protection and safeguard action (i.e. the value is high and could go to very high). It is the penultimate line of defence before safety and/or availability are impacted.

Open doors and elevated cabinet temperatures are faults in instrumentation and control equipment which are classed as Severity 1.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 52 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

### **Severity-2 alarm**

This severity level indicates a major fault, a loss of functional redundancy, or that an automated routine is about to be initiated. The corresponding anomaly requires operator action before the equipment reaches its trip point or the automated routine is initiated.

The anomaly is associated with a potential safety or availability hazard. This alarm is the last line of defence before safety and/or availability are impacted, as defined for severities 3 and 4.

### **Severity-3 alarm**

This severity level implies real consequences for safety and/or availability because an equipment item or a function has been completely lost.

This level of severity is used for a serious fault. During normal operating conditions or during incidents, the failure could initiate the safeguards systems and require operator action to avoid trip thresholds being reached. During accidents, the consequences of the failure could affect the safety of the plant or personnel.

### **Severity-4 alarm**

This level of severity implies significant and real consequences for safety that call for operational management for incidents or accidents; Emergency Operating Procedures (EOPs). It covers all alarms that prompt entry into EOP. A severity-4 alarm signals entry into an Incident Condition or Accident Condition and triggers the AD function. Section 4.3.3.3 of this sub-chapter outlines the annunciation function of the AD system and Sub-chapter 18.3 provides a technical description of the Automatic Diagnosis system. Section 4.5 of this sub-chapter discusses how the UK EPR design and operating concepts reduce the potential for misdiagnosis, including the role of the AD).

The protection thresholds that trigger these alarms give the operating team an indication of the initiating event.

Severity-4 alarms also include alarms indicating that the safeguard systems (e.g. Reactor Trip, Safety injection) have been initiated, that electrical power has been lost and/or that thresholds have been exceeded (e.g. increased SG activity, leakage above the threshold specified in the Operating Technical Specifications). Such alarms require EOP.

Fire alarms are not severity-4 alarms: the existence of a fire must be confirmed before entry into EOP. Fire alarms are thus treated separately.

#### **4.3.3.3. Automatic Diagnosis Annunciation**

When the criterion for incident or accident conditions (severity-4 alarm) is met, the Automatic Diagnosis system is activated.

The annunciation function of the AD is in the form of an AD alerting icon on every MCP [PICS] format header which illuminates red and flashes. In addition, there is a specific AD audible alarm.

The operator acknowledges the AD and the icon, which silences the audible alarm and the flashing MCP [PICS] header becomes steady. The operator then uses the AD status display to view the status of the six state functions and obtain information on the strategy to apply (written procedures and links to display formats).

UK EPR	PRE-CONSTRUCTION SAFETY REPORT	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 53 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

In the situation where early entry into the AD is required as a result of the plant entering a Technical Specification condition, but the plant state conditions are not yet degraded, then the operator will trigger AD through a manual input.

The FA3 HFE programme included assessment of alarm system design, in particular the Automatic Diagnosis feature. The results of the FA3 HF supplementary test campaign [Ref-1] concluded that Automatic Diagnosis was applied systematically and with confidence by the operators. It was also concluded that the content of the automatic diagnosis status display was considered sufficient for representation of the state of deterioration of the facility and for becoming aware of the required operating objective. The Automatic Diagnosis breakdown displays were considered easy to use, and supported understanding of the logic behind the AD decision, in the event of AD unavailability.

The UK EPR specific task analyses of post-fault operator actions discussed in section 5 of this sub-chapter confirm that the AD annunciation is compelling, and that the AD overview screen provides clear information and guidance to the operators on the status of the safety functions, and the appropriate strategy to apply.

#### 4.3.3.4. Alarm Philosophy in the State Oriented Approach

Events covered by emergency operation and subsequent actions may trigger numerous alarms. A given alarm can be initiated by pressuriser diverse events sequences with diverse operating concerns. For example, a high pressuriser level can be:

- favourable in Loss of Cooling Accident (LOCA) situation, showing good recovery of primary water inventory;
- misleading in case of pressuriser steam leak, giving the right information (water content in the pressuriser) or an incorrect impression of primary water inventory (vessel may be drained);
- misleading in case of I&C failure, giving erroneous information about plant status.

The UK EPR design and State Oriented Approach include suitable provisions to cope with this diversity of cases and related concerns. All the information necessary to determine and implement the required operating actions is explicitly defined in the Emergency Operating Procedures. This includes both analogue information (values of physical parameters) and logic information (threshold changes, results of synthesis information, including alarms).

Operators use the information in the procedures to perform the checks included in the emergency operating instructions. The subsequent actions are specified in the self contained Emergency Operating Procedures, without any need to apply alarm sheets. The operator is not required to assign priority and respond to individual alarms when operating in the State Oriented Approach. This approach is designed to reduce the potential for the following;

- misdiagnosis (see section 4.5.5 of this sub-chapter for further discussion of how the UK EPR design and operating concept reduces the potential for misdiagnosis);
- a potential delay in the diagnosis and then in the implementation of the strategy relevant to the plant state;
- implementation of low priority or unnecessary actions.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 54 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

As a defence in depth provision, operators or maintenance staff may react to any alarms not explicitly specified in the Emergency Operating Procedures (equipment progressive degradation, e.g. pump bearing temperature), under the following conditions:

- the plant behaviour dynamics enables the management of the alarm;
- the management of this alarm is not incompatible with actions of the ongoing operating procedures strategy;
- staffing (Field Operators) is sufficient to undertake priority workload for Emergency Operating Procedures.

This provides the opportunity for the operator to anticipate the system status and subsequent plant behaviour, and more efficiently utilise available operations and maintenance team resources.

#### **4.3.3.5. MCP [PICS] Alarms**

Alarms are displayed on computerised workstations that are part of the Process Information and Control System (MCP [PICS]) [Ref-1].

If an alarm occurs, the operator is informed via flashing indicators displayed in a specific area (permanent alarm header) of the operational screen. Each level of severity has a different coloured indicator and as noted in section 4.3.3.3 of this sub-chapter there is a specific AD alerting icon.

An alarm is also indicated by an audible signal.

The alarm presentation concept provides a clear visual and auditory alert to the operator.

Using the MCP [PICS], the operator will select one of the alarm indicators to access the list of alarms relating to that indicator's severity level. This list is not permanently displayed. At the operator's request, it appears on the operational screen chosen for a period appropriate to the operator's actions.

#### **4.3.3.6. MCS [SICS] Alarms**

Principles for specifying and handling alarms, including the alarms provided on the MCS [SICS] are defined in [Ref-1]. MCS [SICS] design criteria and alarm requirements are defined in [Ref-2]. These will be updated during the detailed design phase. In the MCS [SICS], alarms are relayed by trans-illuminated alarm tiles, grouped in relevant sections of the panel. The MCS [SICS] uses the same prioritisation system as the MCP [PICS].

MCS [SICS] alarms are not validated against the plant state. With this exception, the principles used to define an alarm, determine its severity and how it is processed are identical for the MCP [PICS], MCS [SICS] and RSS workstations.

#### **4.3.3.7. Alarm sheets**

Each alarm is associated with a one page alarm sheet showing the operator the operational procedure to be followed. In the MCP [PICS] and RSS, the alarm sheet is displayed by a single click on the corresponding line in the list of alarms.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 55 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

The alarm sheets supply the information required to explain unexpected events signalled by an alarm. In particular, they:

- indicate the causes of the alarm, i.e. the fault causing the alarm;
- indicate the operational procedure to be followed. This part of the alarm sheet tells the operator what actions to take;
- indicate the functional consequences of the fault. The “Consequences” section lists the consequences of the fault and the associated risks;
- allow the operator to revert to control views. The “Views” section of the alarm sheet enables the operator to switch to control or status views using navigation buttons, to check automated actions and to execute the actions defined in the operational procedures.

When MCP [PICS] is unavailable (see section 4.3.2.2.1 of this sub-chapter), operating staff use MCS [SICS] and the situation is managed through incident and accident operating procedures (alarm sheets are not used).

Where relevant (internal flooding), the Type C post-fault task analyses discussed in section 5 of this sub-chapter considered the adequacy of alarm sheets for the specific scenarios analysed. Recommendations were made as appropriate and are included in the UK EPR GDA Human Factors Issues Register.

#### **4.3.3.8. Fire Alarms**

Fire alarms are relayed to the fire alarm cabinets.

The fire alarm cabinet normally uses an audible signal for fire alarms that is sufficiently identifiable to alert the operators. This audible signal is very different from the sound used for conventional alarms.

The fire alarm instructions and the specific associated actions are provided in the fire detection panel. The functional consequences of a fire will be processed by functional alarms in the MCP [PICS] or MCS [SICS].

#### **4.3.4. Non-MCR and Local Controls and Indications**

##### **4.3.4.1. HMI in the RSS and TSC**

###### **4.3.4.1.1. RSS**

The HMI in the RSS is designed to enable the operators to bring the reactor to a safe shutdown state and maintain it in that state. Section 4.2 of this sub-chapter discusses the general design and layout of the RSS.

Previous EDF plant series used conventional HMI in the RSS. The UK EPR RSS HMI design incorporates computerised MCP [PICS] workstations similar to those in the MCR including PSOT terminals (see below for more details). The use of MCP [PICS] rather than MCS [SICS] technology as the primary HMI in the RSS improves consistency in operation between the MCR and RSS in relation to previous EDF plant series. The increased functionality associated with use of the MCP [PICS] rather than conventional panels used in previous EDF plant series also means that there should be less need to carry out operations locally.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 56 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

The MCP [PICS] operator workstations in the RSS have the same number of screens and functionality as those in the MCR. The additional workstation has only two screens. It is configurable only in supervision mode and enables the Shift Manager / Safety Engineer to monitor the state of the plant without interrupting the operating team. The workstation may be shared by the Shift Manager / Safety Engineer as dictated by the operational requirements.

The two PSOT terminals in the RSS have the same functionality as those provided in the MCR. As noted in section 4.2 of this sub-chapter, the RSS has no Plant Overview Panel.

The design and operating principles (switching between the MCR and the RSS in particular) are discussed in Sub-chapter 7.2. The transfer sequence includes manual trip of the reactor operations prior to MCR evacuation. In normal operation, the RSS workstation screens are in standby mode so they can be rapidly brought into operation. Upon arrival at the RSS, the operators transfer control to the RSS by turning six rotary switches from MCR to RSS positions (three to inhibit the MCS [SICS], three for Severe Accident Panel inhibition). These six switches are located in the RSS [Ref-1]. The MCP [PICS] workstations can be locally disconnected from the terminal bus by a Field Operator once a decision to transfer to the RSS has been made in order to avoid spurious operation from the MCP [PICS] [Ref-1]. The operators will then monitor and control the transition of the unit to a safe shutdown state using the MCP [PICS] remote shutdown screens.

The procedures for MCR to RSS transfer, and subsequent operation from the RSS, will be developed and validated during the detailed design phase.

#### **4.3.4.1.2. HMI in the Technical Support Centre**

The TSC has a workstation identical to the Shift Manager workstation in the MCR. All the information held in the MCP [PICS] is also available on the screens in the TSC but without the control functions.

The TSC operator workstation is not operational except in a situation where an emergency response team is needed.

#### **4.3.4.2. Local-to-plant control and display provisions**

Computerised workstations connected to the MCP [PICS] and configured in supervision mode may be installed outside the MCR to supply information to members of the operating team located outside the MCR (for example personnel responsible for isolating equipment). Such workstations will be installed in appropriate locations (for example the Permit Room).

Manual controls and displays are also installed outside the MCR, local-to-plant. Examples of plant locations with local controls and displays include the effluent treatment building and diesels building.

Local-to-plant manual actions are carried out by Field Operators at the request of the MCR operator. Local controls fulfil functions that:

- are independent of the MCR, or;
- are autonomous, requiring only few control actions, and no or very limited coordination with the MCR; and;
- require no immediate manual control in the event of system failures or incidents.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
		PAGE : 57 / 130
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	Document ID.No. UKEPR-0002-181 Issue 06

Although these functions are not controlled manually from the MCR, safety significant local-to-plant actions can be monitored from the MCR.

Suitable controls (and associated facilities, where applicable) are provided in support of specific claims for local manual action, for example ASG [EFWS] tank cross connection, and start up of the Station Blackout Diesels.

Analysis of local-to-plant actions has been carried out, where applicable, as part of the task analyses of post-fault (Type C) claims on operator action described in section 5 of this sub-chapter. The analyses demonstrate that in most cases local-to-plant actions are not necessary to achieve a claimed action. The analyses also demonstrate that safety significant local-to-plant actions can be monitored from the MCR, either directly, or by monitoring associated system parameters. Full substantiation of local-to-plant actions claimed in the safety case will be carried out during the detailed design phase when the design, procedures and relevant aspects are sufficiently advanced.

The future licensee is responsible for ensuring that HF requirements are incorporated into the detailed design of local-to-plant controls and displays, and substantiation that the detailed design supports specific claims on local-to-plant operator actions.

Sub-chapter 7.2 discussed the Priority and Actuation Control System (PACS), which controls and monitors each actuator under all plant operating categories. This I&C system also selects the highest priority command in the case of simultaneous commands on different systems or locations (e.g. MCR and local-to-plant).

#### **4.3.5. Human Factors Validation of the HMI Design**

The FA3 HFE programme described in section 3 of this sub-chapter included HF studies to support the validation of UK EPR Human-Machine Interfaces in particular for the principal HMIs involved in monitoring and controlling nuclear safety. These studies are noted in the sections above in relation to the various aspects of the HMI design.

Key aspects of the MCR HMI design have also been assessed and substantiated to a level appropriate to the generic design phase, through the UK EPR specific task analyses of post-fault claims on operator action, which are discussed above and in section 5 of this sub-chapter.

### **4.4. OPERATING TEAM STAFFING CONCEPT**

***The operating team staffing concept applied in the generic design supports the reliable operation of the plant in all operating modes and categories.***

This section provides arguments and evidence to support the above claim. As described in section 3 of this sub-chapter, OPEX from the existing EDF fleet has been used to develop guiding principles for the organisation of the FA3 operating team (see section 4.4.1 of this sub-chapter). The operating team composition and minimum shift complement has been established (see section 4.4.2 of this sub-chapter). Roles and responsibilities of the team members for the various operating categories have been defined (see section 4.4.3 of this sub-chapter). Human Factors studies have also been carried out to validate the operating team staffing concept (see section 4.4.4 of this sub-chapter).

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 58 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

The FA3 operating team staffing concept described in this section is indicative for the UK EPR. The future licensee is responsible for defining the specific requirements relating to the composition, roles, responsibilities and competencies of the MCR team. However, the substantiation of the Human Based Safety Claims in the UK EPR safety case for the generic design, and reported in section 5 of this sub-chapter, is based on the FA3 operating team staffing concept. Changes to this concept would therefore require review and consideration.

The staffing concept presented relates to the Main Control Room. The future licensee is also responsible for the defining staffing and competence requirements for the entire plant as part of the development and ongoing management of the nuclear baseline required by the Nuclear Site License.

#### **4.4.1. Guiding Principles**

Guiding principles for the organisation of the FA3 operating team have been developed based on OPEX from the EDF fleet [Ref-1]. These are as follows:

P1: Suitable workload in all operating modes; each member of the team should be kept reasonably occupied, with neither too much nor too little to do.

P2: Clear assignment of duties to each individual; activities performed by the team are allocated to ensure clear and comprehensive coverage.

P3: EPR process functions reduce the scope for manual action and set up a line of defence against human errors.

P4: The organisation must allow additional lines of defence against human errors to be put in place in the form of checking and verification.

P5: Consistency in the team organisation between the different operating modes where possible.

The principles outlined above have been used to support the development and validation of the FA3 operating team staffing concept.

#### **4.4.2. Operating Team Composition and Minimum Shift Complement**

##### **4.4.2.1. Operating Team Composition**

The FA3 operating team staffing concept consists of an Operator Action (OA), Operator Strategy (OS), Shift Manager (SM), Safety Engineer (SE) and an Operational Safety Officer and Field Operators. The roles and responsibilities of the team members during normal, emergency and Severe Accident operation are summarised in section 4.4.3 of this sub-chapter and in [Ref-1].

The N4 series operating team staffing concept included a primary and a secondary side operator. OPEX identified some disadvantages with this organisation. These included difficulties maintaining an overview of operating activities, and communication and co-ordination of primary and secondary side procedural strategies. In addition, in most cases there was an imbalance in workload between the primary and secondary side operator in emergency operating scenarios.



<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 59 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

The OA and OS concept was developed to address the disadvantages identified during the OPEX phase (see section 3 of this sub-chapter). It also provides a line of defence against potential human errors in the form of OS monitoring of OA decisions and actions. This is in accordance with principle P4 outlined in section 4.4.1 of this sub-chapter above. In the OA/OS concept, both operators work in co-ordinated manner, using one strategy covering both primary and secondary side, with clearly allocated roles and responsibilities, and a shared understanding of plant state. The OA is responsible for implementing actions, and the OS maintains a global overview of the strategy and monitors OA actions and decisions. Both the OA and OS are fully qualified operators.

The FA3 2005 supplementary test campaign discussed in sections 3 and 4.4.4 of this sub-chapter included consideration of team organisation through simulations of emergency operating scenarios [Ref-2].

**4.4.2.2. Minimum Shift Complement**

The FA3 minimum shift complement has been defined as 1 Operator Action (OA), 1 Operator Strategy (OS), 1 Shift Manager, 1 Operational Safety Officer (responsible for equipment lockout/tagout), and Field Operators (number to be defined) [Ref-1]. The design basis scenario for the FA3 MCR minimum complement is an emergency operation transient plus fire and injured personnel. The staffing requirements outlined above are considered to be the minimum complement for the FA3 Initial Reference Design; however additional staff may be required to supplement the team for periods of known high workloads, such as outages [Ref-1].

The minimum complement for the UK EPR assumed in the Type C post-fault task analyses is 1 Operator Action (OA), 1 Operator Strategy (OS), 1 Shift Manager and 1 Safety Engineer, who arrives at the MCR within 40 minutes of being requested. Field Operators are also required to perform local-to-plant activities.

The future licensee is responsible for further definition and validation of the UK EPR staffing requirements, including requirements for Field Operators and other personnel required to ensure safe operation. The UK EPR Type C task analyses of post-fault scenarios discussed in section 5 of this sub-chapter provide an input to this process as they identify potential high MCR workload scenarios and issues relating to task allocation for specific Type C HBSCs.

**4.4.3. Roles and Responsibilities**

The roles and responsibilities of each member of the operating team have been defined. In principle, the plant is run by two operators (Operator Strategy - OS and Operator Action - OA) and a Shift Manager who is the team leader [Ref-1]. The Shift Manager (SM) is equivalent to the Shift Supervisor, which is the terminology used in some International Standards and guidelines (e.g. NUREG 0711). This team organisation has been subject to high level evaluation for Flamanville 3 [Ref-2] [Ref-3]. This organisation:

- permits a division of work and responsibility to prevent task-overloading of individual operators;
- provides human redundancy and diversity;
- provides coverage for tasks that are additional to operational management, such as communication, interfacing with maintenance and periodic testing, and;
- ensures sufficient personnel are available should multiple failures occur.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 60 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

The responsibilities of each operating team member for normal, emergency and Severe Accident conditions are outlined below. This is based on the FA3 Initial Reference Design and is indicative for the UK EPR. The roles and responsibilities outlined below should therefore be reviewed and developed during the detailed design phase.

#### **4.4.3.1. Operators**

##### **4.4.3.1.1. Normal operation**

The Operator Action performs actions on the process relating to the application of operating procedures, alarm sheets or test procedures.

The Operator Strategy (OS) oversees the planned operating strategy, takes charge of a limited number of actions, monitors the process to attain the operating objective and/or maintain current status, and diagnoses deviations.

When the plant is running, the tasks of the operators are to:

- perform (or request) manual actions required to start up or shut down or change the configuration of plant systems;
- monitor the safety and availability of the plant from parameters and information supplied by the information systems;
- perform checks and periodic tests to ensure that all the safety systems are fully available;
- take corrective action, in addition to the automated actions, should an equipment item malfunction, or an unforeseen incident occur;
- request corrective actions by Field Operators or maintenance personnel if actions initiated from the MCR are insufficient;
- account for equipment unavailability during maintenance and operation, and make provision to configure the systems or other actions necessary to ensure that the plant functions safely, and in compliance with the technical specifications;
- perform equipment re-qualification (after maintenance operation) in collaboration with Field Operators.

##### **4.4.3.1.2. Emergency Operation**

All activity in emergency operation is undertaken by application of State Oriented Approach procedures, which provide clear, prescriptive instructions to the operator.

- Operator Action activities (OA):
  - performs action in accordance with the strategy. This includes applying methods and operating instruction sheets using command and status views (Action);
  - reports to the Operator Strategy on the execution of these actions. (Communication);
  - requests Field Operators to perform local-to-plant actions (Communication);

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 61 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

- performs first-level monitoring of systems (Monitoring).
- Operator Strategy activities (OS):
  - checks the strategy to be applied. The decision is normally made on the basis of the diagnosis performed by the AD function which uses plant status information to determine the optimum recovery strategy. The OS is also alerted by the system if the status of the AD changes (Action);
  - requests the Operator Action to perform actions applying the appropriate operating method for the strategy (Communication);
  - checks to ensure that actions required by the method have been performed correctly (Checking);
  - performs monitoring tasks to achieve operating objectives with the resources available on the basis of the stated priorities, using synthesis information and important action alerts indicated on the status view (Monitoring).

#### **4.4.3.1.3. Severe Accident Operation**

A discussion of Severe Accident operation is provided in Sub-chapter 18.3. The tasks of the operators are to;

- enter Severe Accident procedures on request of Shift Manager when agreed by the Emergency Controller<sup>1</sup>;
- perform the immediate actions identified in the Severe Accident management documentation;
- monitor and assess plant status in accordance with the Severe Accident management documentation;
- communicate plant status to the Shift Manager who is responsible for liaison with the Emergency Controller and TSC;
- take actions to implement strategies for accident mitigation when directed by the TSC after authorisation has been given by the Emergency Controller.

The specific allocation of tasks between the OA and OS will be defined by the future licensee.

#### **4.4.3.2. Shift Manager**

##### **4.4.3.2.1. Normal Operation**

By delegation of the Plant Director, operational responsibility for running the units and maintaining them at their safety level rests with operational line management. The Shift Manager (SM) is the permanent operational line management representative reporting to the Plant Director or their on duty deputy. The Shift Manager is responsible for the management of the team.

<sup>1</sup> This function is ensured by Plant Director or his/her delegate

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 62 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

The Shift Manager on duty keeps track of all operating activities to ensure compliance with safety requirements. The Shift Manager monitors operation and ensures that it is consistent with the plant's safety and availability principles. The Shift Manager is claimed as a line of defence against operator error since they monitor and oversee MCR team activities. They also ensure that actions of the maintenance team are consistent with the diagnostics performed by the operators.

The Shift Manager decides if intervention is necessary, authorises the maintenance work and periodic tests, launches equipment isolation activity and issues the work orders. The SM is responsible for assessing the safety of the units. These duties may not be delegated.

#### **4.4.3.2.2. Emergency Operation**

The Shift Manager (SM):

- checks to ensure that the Operator Strategy has chosen the correct strategy, and that the key points of this strategy are in line with plant status. The SM also has the automatic diagnosis function and status displays, plus the method (Checking). They may ask for the strategy to be changed, if necessary;
- applies Safety Engineer (SE) procedure for short term (before SE arrival);
- informs the Plant Director or their on-duty deputy if there is an incident/accident;
- co-ordinates MCR team activities and communications;
- communicates with the TSC and the Emergency Controller;
- implements the fire response measures.

#### **4.4.3.2.3. Severe Accident Operation**

In Severe Accident conditions, the Shift Manager;

- applies the Shift Manager procedures for Severe Accident conditions;
- applies Safety Engineer (SE) procedure until the arrival of the SE;
- relays directions and advice from the TSC, and authorised by the Emergency Controller, to the MCR team;
- communicates plant status and MCR activities to the TSC and the Emergency Controller via regular written and verbal progress reports.

#### **4.4.3.3. Safety Engineer**

##### **4.4.3.3.1. Normal Operation**

The Safety Engineer (SE) is responsible for verifying the safe status of the units. The SE on duty performs a daily review of operating parameters and conditions. In normal operation, the SE performs a separate analysis of the situation to be contrasted with the team diagnosis submitted by the SM. The SE performs verifications according to a schedule or on their own initiative, to be in a position to make an objective assessment on the safety status of the unit.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 63 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

#### **4.4.3.3.2. Emergency Operation**

The SE is called to the Main Control Room whenever an event meeting the defined criteria is detected. This includes any situation requiring application of incident or accident instructions. The SE must be able to reach the MCR within 40 minutes of being requested [Ref-1].

During emergency operation, the SE independently verifies results of the team's activity, applies specific instructions (paper based Safety Engineer procedure which is applied on the MCS [SICS] panel) and requests a change of strategy, if necessary.

#### **4.4.3.3.3. Severe Accident Operation**

The SE performs the following specific functions during Severe Accident operation;

- provides information to the Emergency Controller when the criteria to enter Operating Strategies for Severe Accidents (OSSA) is reached (this is specified in the continuous state monitoring procedure which is applied by the SE on the MCS [SICS] panel);
- independent monitoring and evaluation of plant status using the MCS [SICS], including surveillance of critical safety functions.

#### **4.4.3.4. Operational Safety Officer**

The Operational Safety Officer is responsible for equipment lockout/tagout and is in charge of emergency response for fire-fighting and assistance to injured personnel in both normal and emergency situations.

#### **4.4.3.5. Additional temporary staff**

As previously mentioned in section 4.4.2 of this sub-chapter, depending on the state of the plant, the operating personnel referred to above are supplemented by others from a variety of disciplines, including additional operators during commissioning or outages, automation technicians, and plant-based operations personnel. Some of these staff are only required on a temporary basis.

### **4.4.4. Human Factors Validation of the Operating Team Staffing Concept**

#### **4.4.4.1. FA3 HFE Programme**

As described in section 3 of this sub-chapter, the FA3 2005 supplementary test campaign included evaluation of different MCR team organisation arrangements through simulations of emergency operating scenarios [Ref-1]. The tests were carried out with 4 operations teams, representing three series within the French nuclear fleet (900MW, 1300MW and N4). The three scenarios simulated were LOCA, Main Steam Line Break (MSLB) plus Steam Generator Tube Rupture (SGTR) and spurious reactor trip followed by a primary break. Some recommendations were made relating to the division and assignment of tasks to ensure appropriate balance of workload between MCR team members.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 64 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

#### 4.4.4.2. UK EPR Specific HF Analyses

The results of the Type C post-fault task analyses discussed in section 5 of this sub-chapter demonstrate that the operating team staffing concept applied in the generic design supports reliable performance of post-fault actions. The task analyses considered OA tasks in detail and OS and SM at general role level. The task analyses confirmed that the roles and responsibilities of the operating team members are defined and allocated (including the allocation of tasks to the OA and OS). The assignment of specific responsibilities for response implementation, peer checking and diverse independent monitoring via the MCS [SICS] panel supports the prevention and recovery from errors relating to misdiagnosis, violations, and errors associated with response implementation (errors of commission or omission).

The OS, SM and SE roles provide important detection and recovery mechanisms for human failure events. In particular, the analyses support the claim that the OS provides a line of defence against potential human errors in emergency (incident and accident conditions). This is achieved through the OS role of checking that the correct strategy is applied and monitoring key actions and decisions taken by the OA. This aspect of the OS role was demonstrated during simulator observations undertaken as part of the task analyses (see section 5.3 of this sub-chapter for more details).

For most scenarios, the level of workload experienced by the OA and OS was considered to be manageable. Some high workload scenarios for the OA were identified through the task analyses (for example, certain loss of offsite power and steam generator tube rupture scenarios). Recommendations have been made to ensure that workload is appropriate during such scenarios (e.g. further consideration of the allocation of tasks between MCR team members, allocation of secondary tasks such as co-ordination of Field Operators). Management of high workload scenarios requires consideration regardless of the staffing strategy selected. The issues identified through the analyses do not relate to the generic design or allocation of safety functions, and will therefore be addressed as part of the detailed design phase. They are captured in the UK EPR GDA Human Factors Issues Register.

The future licensee is responsible for carrying out further validation of the operating team staffing concept as part of the UK EPR HFE programme for the detailed design phase.

#### 4.5. UK EPR PROCEDURE CONCEPT

***The UK EPR procedure concept applied in the generic design supports reliable human performance during activities that could impact on safety. In particular, the State Oriented Approach supports reliable fault diagnosis and response.***

This section provides a summary of the UK EPR procedure concept, along with arguments and available evidence to support the above claim.

The FA3 Initial Reference Design operating procedure concept described in this section is indicative and could be adapted by a future licensee. However, the State Oriented Approach is integral to the substantiation of Human Based Safety Claims (see section 5 of this sub-chapter). Changes to this concept would therefore require review and consideration.

The future licensee is responsible for the detailed design of procedures (both paper-based and computerised). This includes specifying the process for development, verification, validation of procedures, development of a style guide to provide a consistent approach to procedure format and content, and for related policies and processes such as procedure use and adherence, and ongoing review and updating of procedures.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
		PAGE : 65 / 130
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	Document ID.No. UKEPR-0002-181 Issue 06

Sub-chapter 18.3 provides a description of the State Oriented Approach. It also includes a discussion of Severe Accident operating principles, documentation and criteria for declaring a Severe Accident. Sub-chapter 18.2 includes a discussion of normal operating documents, and interfaces between normal and abnormal operating procedures. Maintenance and testing procedures are discussed in Sub-chapter 18.2.

#### **4.5.1. Summary of the UK EPR Procedure Concept**

The FA3 Reference Design procedure concept includes a comprehensive set of procedures to support the reliable performance of safety related tasks.

The structure of the FA3 Reference Design operating procedures is an evolution of the N4 and other series of French NPPs.

The FA3 Reference Design operating procedures consist of a set of operating rules and instructions. This terminology is used for normal and emergency operation (incidents and accidents) [Ref-1]. Sub-chapter 18.1 - Figure 2 shows the types of operating procedures.

The operating rules specify the operational objectives, principles, logic, chronology and justification. The operating instructions are written based on one or more operating rules and formalise the step-by-step procedure that the operator must follow.

The operating instructions comprise the paper-based operating methods, together with the operating instructions available on screen of the computerised workstations (for the MCP [PICS]), and on paper for the conventional workstations (MCS [SICS]).

The operating method describes the strategy determining the action to take. This depends on predetermined criteria relating to physical states or the status of components (the actions are described in the procedure). The strategy is generally presented as a set of comprehensive logic diagrams plus references to the relevant process status view and the procedures to use both to track the main parameters that could change, and to display the correct operational views, so that the operator may intervene in the process. For the Operator Action (OA), the operational method specifies the actions and checks to be performed. For the Operator Strategy (OS), the operating method includes a logic diagram of the OA actions, significant surveillance actions and a global view of the operating strategy. Local action sheets are also provided. These are paper-based documents which define actions to be performed outside the MCR by Field Operators.

Operating Instruction Sheets are computerised via the MCP [PICS]. Operating Instruction Sheets are displayed as text and present a chronological sequence of actions to be performed by the OA (checking and controlling components). Hyper-links are provided which take the operator directly to control and status displays used to perform actions, and include reference to relevant local action sheets.

The structure described above applies to normal operation as well as emergency operation (State Oriented Approach) and Severe Accident operation.

The organisation of procedures in terms of computer based and paper based copy instructions has been designed to support reliable performance and specific operating team roles. The paper based procedures define the strategy, as well as local-to-plant actions which require paper based documentation. The computer based procedures are used for detailed action implementation. Consideration has been given to ensuring that the procedures support specific MCR team roles in emergency conditions (see section 4.5.3 of this sub-chapter).

UK EPR	PRE-CONSTRUCTION SAFETY REPORT	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 66 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

N4 OPEX for normal operation identified that the recording and annotation of actions are important for place-keeping in the procedures and for future reference purposes. The UK EPR operating methods and instruction sheets, whether paper-based or displayed on the screen, will provide check-off and annotation functions. For paper based instructions, this is achieved by tracing the path followed and annotating the paper copy. For computerised instructions check-off boxes on screen and an annotation function are provided. These features support awareness of the state of progress through the instructions and reduce the likelihood of accidentally skipping a step or making an interpretation error [Ref-2].

Paper-based instruction sheets serve as back-up to screen-based instruction sheets. Paper-based versions of operating procedures are provided in the MCR in the event of a computer failure.

Adequate space is provided at the appropriate workstations in the Main Control Room and remote shutdown station for operators to use paper based procedures when required.

As noted in section 3 of this sub-chapter, the high level design principles for the procedures were defined by multidisciplinary WGs. The input data used by these WGs was provided by OPEX review and by the Operation Department requirements.

### 4.5.2. Normal Operating Procedures

The scope of normal operating procedures for the FA3 Reference Design includes at-power operations and normal scheduled operating transients. Normal operating procedures also include specific procedures and alarm sheets for conditions that do not require the use of emergency (incident/accident) operating procedures. Examples include equipment failure, power manoeuvres, and flooding. Alarm sheets are presented via the MCP [PICS] to provide rapid access to alarm information. Section 4.3 of this sub-chapter provides a discussion of the alarm system design, including alarm sheets.

The operating method/instruction sheet division allows the future licensee to manage the order in which the instruction sheets are performed according to the status of the equipment and outage activities that are in progress or scheduled [Ref-1].

OPEX has been used to make improvements to the design of normal operating procedures. For example, the automatic monitoring of operator actions implemented on the N4 series is not included in the EPR design. This reflects the design principle that the computerised system should provide operating staff with the means to perform their job responsibly, allowing operators to perform and co-ordinate the activities required by their role [Ref-1].

Rules for drafting normal operating rules have been developed [Ref-2]. Design rules for operating instructions have also been produced which specify the process and format for producing operating instructions [Ref-3].

### 4.5.3. Emergency Procedures

#### 4.5.3.1. Overview of the State Oriented Approach

This section discusses the State Oriented Approach in terms of how it supports reliable operator performance, and the basis for the approach.

A description of the technical considerations relating to the use of the State Oriented Approach and the Automatic Diagnosis system is provided in Sub-chapter 18.3.



<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
		PAGE : 67 / 130
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	Document ID.No. UKEPR-0002-181 Issue 06

The SOA consists of a limited set of strategies to be implemented during emergency operation of the plant in order to provide a strategy for responding to an emergency regardless of the initiating event or sequence of events that led to this state. The SOA considers six state functions, each comprising of multiple physical parameters that contribute to defining the plant status at any given time. The SOA strategies therefore relate to the necessary response to such state functions, depending on their status, allowing the operator to follow the correct course of action. The strategies are described in Sub-chapter 18.3. The operator is provided with a dedicated MCP [PICS] screen for each operating method (strategy), grouping all information necessary to support the performance of required tasks, including hyperlinks to the relevant operating instructions.

The SOA is used in all emergency (incident and accident) situations unless Severe Accident conditions (i.e. core damage) occur (see section 4.5.4 of this sub-chapter for a discussion of Severe Accident procedures). Section 4.5.5 of this sub-chapter includes a discussion on how the design and procedure concept reduces the potential for misdiagnosis, including scenarios involving failure of the Automatic Diagnosis function.

The SOA procedures are based on those applied in the existing EDF fleet. The approach was originally developed by EDF and Framatome following the Three Mile Island accident, the objective being to provide a robust response to faults that are beyond design basis or that represent an accumulation of faults. When operating in the State Oriented Approach, required operator responses are based on the continuous monitoring of a limited set of key safety functions, regardless of the sequence of failures or events that led to the state.

Entry into the State Oriented Approach is signalled by a severity-4 alarm, which initiates the Automatic Diagnosis (as described in section 4.3 of this sub-chapter and Sub-chapter 18.3). Upon receipt of the Automatic Diagnosis, the operating team enters the State Oriented Approach, which includes a paper-based procedure for each strategy. The AD is a diagnostic support feature; in accordance with the principles outlined in section 4.1.1.2 of this sub-chapter, the operator remains in charge of the plant.

The structure and content of the procedures has been tailored to the operating team staffing concept discussed in section 4.4 of this sub-chapter. The OA and OS use separate versions of the same State Oriented Approach procedure, which are colour coded to distinguish between the OA and OS versions. The OA version describes the actions to take and the OS version defines the monitoring and surveillance of OA actions. The procedures are paper-based A3 size documents, which include logic diagrams (flow charts).

Procedures for the MCP [PICS] include references to the appropriate MCP [PICS] display formats. The MCP [PICS] paper based strategy procedures direct the operator, where appropriate to computerised instruction sheets on the MCP [PICS]. Procedures for MCS [SICS] operation include reference to the appropriate control/instrumentation of the MCS [SICS]. The MCS [SICS] paper based strategy procedures direct the operator, where appropriate to paper-based instruction sheets.

There is also a specific procedure applied by the SE (or SM if the SE is not immediately available in the MCR). This focuses on monitoring the key plant parameters on the MCS [SICS].

The State Oriented approach is designed to support situational awareness and shared understanding of the overall strategy being applied. There is one procedure per strategy to provide the operating team with a global approach to the strategy for fault management, rather than separate procedures for primary and secondary side actions. This also supports communication and collaboration between the various members of the operating team.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
		PAGE : 68 / 130
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	Document ID.No. UKEPR-0002-181 Issue 06

#### **4.5.3.2. Development, Verification and Validation of Emergency Operating Principles and Procedures**

##### **4.5.3.2.1. FA3 Initial Reference Design**

Emergency operating principles were defined by a multidisciplinary working group, including Human Factors specialists. The role of the HF specialists in the working group was to ensure that the design of the EOPs reflected the positive and negative experience feedback relating to the use of EOPs, and was adapted to suit the EPR design.

An initial assessment of the principles defined by this working group was conducted in 2005 [Ref-1] as detailed in section 3.1.3.3 of this sub-chapter.

Following this assessment, several principles were subject to further validation including, for example, the Automatic Diagnosis principle and the emergency procedures structuring principles [Ref-1] as detailed in section 3.1.3.3 of this sub-chapter.

The teams considered that they had a good view of the state of deterioration of the facility using the Automatic Diagnostics display. The results of these HF tests were presented in Technical Reviews (see section 6 of this sub-chapter on HF Process Assurance).

The process for developing the state oriented approach procedures and its interfaces with the equipment qualification process has been defined for the FA3 Reference Design [Ref-2]. This includes Human Factors verification and validation of the procedures, which has been underway since 2008. The contents and structure of emergency operating rules and methods have also been specified [Ref-3] [Ref-4].

##### **4.5.3.2.2. UK EPR specific HF analyses**

The post-fault (Type C) task analyses reported in section 5 of this sub-chapter included consideration of the appropriateness of the preliminary FA3 procedures used for response to the fault scenarios. Specific procedural factors that were considered as part of the analyses included navigation within and between procedures, completeness and clarity of procedural guidance. The analysis process also included observations of use of SOA approach in conjunction with use of computerised operating instructions on the MCP [PICS], and the status and control screens used to support monitoring and control actions specified in the procedures.

The results of the analyses provide support for the emergency operating procedure concept (i.e. SOA) and procedure design principles applied in the generic design. The provision of specific Operator Strategy procedures to monitor implementation of the Operator Action procedures supports error prevention, detection, and to some extent recovery. The concept of 'looping' in the procedures (i.e. making several passes through the procedure) also provides a mechanism to detect and recover from potential human errors. The following features which support reliable performance were identified through the analyses; the use of colour coding for differentiation between different versions of the SOA procedures, clarity of procedures in relation to actions required and the location in which to perform them, explicit statements for a checking or verification action to take place, and clear indication in the Operating Instruction Sheets as to what procedure is/should be implemented.

Recommendations for the detailed design of paper based and computerised procedures have been made where appropriate and are captured in the UK EPR GDA Human Factors Issues Register for consideration as part of the procedure development process. In some cases, the computerised operating instructions were not implemented on the MCP [PICS] due to status of the design. These and other assumptions relating to procedures are also identified in the task analysis reports and UK EPR GDA Human Factors Issues and Assumptions Registers for consideration during the detailed design phase.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
		PAGE : 69 / 130
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	Document ID.No. UKEPR-0002-181 Issue 06

Human Factors verification and validation of procedures is an iterative process. The future licensee is responsible for further verification and validation of the Emergency Operating Procedures, including simulator validation at the end of the design process.

#### **4.5.4. Severe Accident Guidelines**

Whereas Emergency Operating Procedures focus on safeguarding core integrity, priorities for Severe Accidents are directed towards limiting radioactivity releases into the environment and preserving containment integrity. This involves implementation of certain dedicated systems and mitigation strategies. For such highly improbable conditions, the operation of the unit may also require unusual operational actions which might be contrary to the principles of operation in normal or emergency conditions. Dedicated documentation is therefore applied to Severe Accident management.

The criterion for switching from emergency operation to Severe Accident operation is a Core Outlet Temperature greater than 650°C. In some instances, where Core Outlet Temperature is unavailable, containment dose rate will be used as switching criterion.

The SE procedures for continuous state monitoring, applied on the MCS [SICS], will guide the SE to check the Enter OSSA criteria. Whatever path the SE takes through the procedures, the SE will always be directed to the reorientation section which contains the criteria. This is an important error recovery mechanism for application of the OSSA entry procedures.

The SE has two procedures for continuous state monitoring; one for closed Reactor Coolant System (RCP [RCS]) and another for open RCP [RCS]. It is assumed that both Enter OSSA criteria (Core Outlet Temperature and containment dose rate) will be checked in both SE procedures for continuous state monitoring, as is the case for the FA3 procedures. This takes away the negative consequences for the Enter OSSA task from the potential error of the SE to start the wrong monitoring procedure.

Once the OSSA entry criterion is reached, the required action is for the emergency organisation to start the application of OSSA guidelines. This is achieved by the SE detecting the OSSA entry criterion and the EC taking the decision to start OSSA. The presence of OSSA entry criterion is communicated to the EC, and the decision to enter OSSA is then communicated to the operating team by the SM under instruction from the EC.

The detection of Enter OSSA criteria is the task of the SM before the arrival of the SE at the MCR. After SE arrival, the SM provides an error recovery mechanism. Once transition is made to OSSA, guidance is provided to MCR for performing systematic actions, known as "immediate actions". These actions, performed by the operators on entry into or during the use of Severe Accident management guidance, do not require evaluation from emergency response teams. After the end of the "immediate actions" the emergency response team will suggest some "delayed actions". The Emergency Controller will validate mitigation strategies by the local and national emergency response teams and instruct the emergency operating team in the MCR to apply the recommendations made.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 70 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

Analysis of Severe Accident Human Based Safety Claims, including the Emergency Operating Procedures used has been conducted as part of the task analysis programme of Type C HBSCs (see section 5 of this sub-chapter). Severe Accident procedures are not yet developed for the UK EPR and the analysis performed was based on FA3 procedures, which are currently under development. The analyses concluded that appropriate procedural support was provided, and that the procedure concept supports reliable performance of the claimed actions. Features of the procedures that support reliable task performance were identified, for example, regardless of the route taken through the procedures, the SE is always directed to the criteria for OSSA entry. Detailed procedure design issues identified through the analyses have been recorded in the UK EPR GDA Human Factors Issues Register. These relate to aspects such as the clarity of certain procedure steps and verification requirements and will be addressed during the detailed design phase as part of ongoing procedure development.

#### **4.5.5. Misdiagnosis Potential**

***The risk of misdiagnosis is minimised by the State Oriented Approach, Automatic Diagnosis, operating team organisation and specific design features.***

An assessment of the potential for and defences against misdiagnosis has been carried out as part of UK EPR specific HFE activities to demonstrate that the potential for misdiagnosis is minimised at the generic design phase and is reported in [Ref-1]. This included consideration of misdiagnosis potential in relation to:

- the initial selection of an appropriate post-fault response strategy;
- the need to exit or change the post-fault response strategy;
- selecting appropriate means to achieve the safety related functions required for the post-fault response.

The methodology included the following steps;

- definition of a set of generic post-fault operator diagnosis tasks conducted in the MCR;
- analysis of each task to identify all credible misdiagnosis errors and their antecedents;
- identification of the UK EPR features that serve as barrier or recovery mechanism, to mitigate misdiagnosis for each antecedent;
- derivation of safety arguments based on these features, which link evidence of the UK EPR feature to each claimed barrier / recovery mechanism.

The assessment concluded that risks from misdiagnosis are demonstrably ALARP for the GDA phase. The EPR incorporates several lines of defence to mitigate the potential for misdiagnosis.

The lines of defence common to MCP [PICS] and MCS [SICS] identified through the assessment include the following [Ref-1];

- the provision of clear tactical level information (information used to implement the required operator response) provides an important barrier to many of the potential antecedents to misdiagnosis error and is achieved through features of the HMI such as hyperlinks to instruction displays, clear labelling and identification of systems/components/trains on MCP [PICS], dedicated status displays for each strategy,

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 71 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

- clear and appropriate naming of the SOA strategies and unique identifiers for each SOA strategy;
- the information for transition between Incident Condition strategies and between phases of strategies (all post-fault categories) is clearly provided. Each procedure has a dedicated MCP [PICS] status display which includes hyperlinks to related screens needed to implement the procedural actions;
- cyclic procedures (looping through the procedures) provide a mechanism for misdiagnosis detection and recovery;
- the OS, SE and SM roles provide an error prevention, detection and recovery contribution. The OS carries out formal peer checking of OA actions as defined in the procedures; the SM maintains oversight of plant conditions and the implementation of the post-fault response provides a mechanism for detecting the occurrence of, and the recovery from, potential operator error, including misdiagnosis; and the SE is to provide independent (as far as is practicable) and diverse (MCS [SICS]-based) recovery mechanism for potential errors, including misdiagnosis, made by the OA / OS;
- threshold changes to key plant parameters are clearly communicated to the operator.

Specific lines of defence on MCP [PICS] identified through the assessment include the following:

- the SOA which removes, by design, the potential for fault scenario initiating event induced misdiagnosis when the AD is functioning. The operator is not required to diagnose the correct strategy in response to multiple events/failures (no interpretation of alarm patterns is required). The diagnosis is carried out by the AD system;
- entry into post-fault conditions is clearly communicated to the operator through the AD system, including compelling auditory and visual annunciation;
- clear indication of the correct strategy to apply is provided to the operator through the AD system;
- an AD breakdown display showing the basis for the AD diagnosis is provided on the MCP [PICS];
- required changes to a strategy when remaining in Accident Condition, and required strategy changes that involve an escalation to the next category of post-fault conditions (e.g. from Incident Condition to Accident Condition), are indicated via the AD; threshold changes to key plant parameters are clearly communicated to the operator;
- AD re-annunciation improves and supports misdiagnosis detection and recovery.

Specific lines of defence on MCS [SICS] identified through the assessment include the following:

- required changes to a strategy when remaining in Accident Conditions, and required strategy changes that involve an escalation to the next category of post-fault conditions (e.g. from Incident Condition to Accident Condition), are indicated via the reorientation phase.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 72 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

The required post-fault operator response is significantly different if AD failure occurs because the input signal failure must be diagnosed. Ensuring that the AD failure is clearly communicated to the operator is key to demonstrating that the associated risk of misdiagnosis has been minimised. The analysis concluded that clear indication is provided to the operator through severity-4 alarms which indicate entry into post-fault conditions, unique AD invalid signal if AD fails, and criteria for transfer to MCS [SICS] are defined (e.g. when the AD is invalid and the flowchart image of the AD logic is also invalid). Adequate procedural support, including dedicated breakdown displays, is also provided. There are also specific procedures for MCP [PICS] failure and diverse HMI to account for the scenario of AD failure (i.e. MCS [SICS]; see section 4.3 of this sub-chapter). In the event of AD Failure, the operator must check the AD breakdown screens at the beginning of each EOP cycle to identify any strategy changes into accident conditions. The operating team roles and responsibilities in situations with AD Failure also minimises the potential for misdiagnosis.

In addition, the assessment, based on qualitative analysis, concluded that the majority of Type C HBSCs were achievable within the time available and that the currently assigned Human Error Probabilities are appropriate. The analysis also identified that the claimed operator actions are supported by procedures, the HMI and peer checking.

HF analysis is an iterative process and further assessment of misdiagnosis potential should be carried out during the detailed design phase.

#### **4.5.6. Violation Potential**

***The risk of deliberate violation in the UK EPR by operators and maintainers is minimised by the UK EPR design and procedure concept.***

The focus at the generic design phase is on design-induced violations. Consideration has also been given to potential violations associated with other factors amenable to analysis during the generic design phase. Consideration has been given to well-intentioned violations (the potential for malicious acts has not been assessed).

Violations are not directly considered in a quantitative manner by the generic design assessment safety case. However, as a direct result of the application of a sound and evolutionary HF design process, based on internationally recognised HF design principles; the vulnerability of the EPR to design-induced violations has been minimised [Ref-1].

As noted in section 1.2 of this sub-chapter, the objectives of the design approach for the UK EPR include supporting positive human contributions and reducing the potential for human errors and design-induced violations.

The user-centred approach described in section 3 of this sub-chapter included extensive use of OPEX. Operators and maintainers from N4 series fleets were interviewed as part of the design requirement capture process and so this has enabled previously encountered design issues that could incentivise violation to be designed out.

The impact of violations for the UK EPR will be significantly mitigated due to the presence of automated plant state monitoring and fault detection to allow rapid detection and recovery from induced fault states. This is ensured due to a number of features, should any degradation of the plant status occur as a result of violation, the state function monitoring would immediately alert the operator and prompt the operator towards appropriate mitigating actions (via the Automatic Diagnosis function). Safety significant operator actions are automatically logged by the system and so will provide a disincentive to violate and the automation of specific safety related actions removes the opportunity to violate the process of action required.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 73 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

The UK EPR task analyses of both pre- and post-fault Human Based Safety Claims include consideration of the potential for violation behaviours. For pre-fault Human Based Safety Claims, the methodology specifically considered the potential for violation and this has been assessed during the Human-HAZOP (Hazard and Operability) process discussed in section 5 of this sub-chapter, to the extent possible at the generic design phase. With regards to post-fault operator Human Based Safety Claims, the task analyses performed have considered the potential for, and consequences of violations. Violation potential has been assessed, where possible, through the consideration of Performance Shaping Factors (such as time available, operational/safety conflicts) and OPEX review. For example, the analyses of feed and bleed HBSCs identified that operators may be reluctant to initiate feed and bleed due to competing operational/safety goals and identified recommendations for consideration during the detailed design phase. The findings and recommendations from the task analyses will be used to support the detailed design so as to ensure that potential violations are appropriately mitigated. Issues and associated recommendations are recorded in the UK EPR GDA Human Factors Issues Register to facilitate this process.

The future licensee is responsible for defining the scope of their safety case with regard to assessment and management of violation behaviours by staff and to determine and mitigate the associated risks.

## 5. IDENTIFICATION AND SUBSTANTIATION OF HUMAN BASED SAFETY CLAIMS

***Human Based Safety Claims (i.e. claims on operator action made in probabilistic and deterministic safety analyses) have been identified and substantiated to a level appropriate to generic design assessment using recognised Human Factors methods.***

The objectives of identification and substantiation of Human Based Safety Claims are:

- to understand the human contribution to plant safety (in terms of reliance on human actions, and the vulnerability of the plant to potential human failure events in pre and post-fault situations), and
- to minimise the associated risks to ALARP for the generic design.

This section discusses the overall risk significance of Human Based Safety Claims in the UK EPR safety case (section 5.1 of this sub-chapter) and provides an overview of the process followed to identify and analyse them (section 5.2 of this sub-chapter). Section 5.2 of this sub-chapter also provides supporting arguments that human actions or omissions that have been assessed to significantly impact on safety (i.e. the HBSCs) have been identified and substantiated at a level appropriate, relative to their safety significance, for the generic design safety case.

HBSCs include both pre-fault (Type A, B) and post-fault (Type C) claims. Type A claims are pre-fault human errors which degrade mitigation system availability. Type B claims are pre-fault human errors leading to an Initiating Event. Type C claims are post-fault claims on operator action. A summary of the process and results relating to the identification and substantiation of Type A, B and C claims is presented for the probabilistic safety case (section 5.3 of this sub-chapter) and deterministic safety case (section 5.4 of this sub-chapter).

A discussion of the pre- and post-fault task analysis results in relation to specific aspects of the UK EPR design and operating concept (e.g. allocation of function, HMI design, operating team staffing concept, UK EPR procedure concept) is included in section 4 of this sub-chapter.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 74 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

## 5.1. OVERALL RISK SIGNIFICANCE OF HUMAN BASED SAFETY CLAIMS

As discussed in Sub-chapter 15.7, the UK EPR assessed overall CDF is low ( $7.1\text{E-}07/\text{r.y.}$ , including preventive maintenance, relative to the safety objective of  $1\text{E-}05/\text{r.y.}$ ). This figure includes the contribution of human error, particularly post-fault human errors (Type C) and pre-fault human errors (Type A) relating to the misalignment of manual valves following maintenance performed either during at-power or shutdown states.

Sub-chapter 15.7 - Figure 3 shows the relative importance of operator error compared to the other systems of the UK EPR in terms of Core Damage Frequency. It notes that the operator has a relative contribution of 23.6%.

Other Type A errors are included in overall failure rates for UK EPR systems derived from EDF databases, rather than explicitly modelled in the PSA. Generally, the initiating event frequencies modelled in the UK EPR PSA are derived from NPP OPEX and reflect both component and human failure events. In general, type B human errors are incorporated into the initiating event frequencies. As noted in Sub-chapter 15.7, unavailability of systems due to corrective maintenance is not currently explicitly modelled in the UK EPR PSA. However, preventive maintenance is modelled using one week unavailability (typically) for each train of the relevant systems over one year. This duration is considered bounding for both preventive maintenance and corrective maintenance, since detailed information on maintenance activities is not available at the generic design phase.

Post-fault claims on operator action (Type C claims) have been identified as part of the revised 2011 PSA and are summarised in [Ref-1]. The PSA includes 8 high risk HBSCs (in terms of their contribution to Core Damage and Large Early Release Frequency). The criteria for risk significance are discussed in sub-section 5.3.3.2 of this sub-chapter.

Risk significant pre-fault HBSCs have been identified through the process described in sections 5.3 and 5.4 and summarised in section 5.2 of this sub-chapter.

The analysis undertaken for the generic design has been proportionate to the potential nuclear safety risk and it is therefore unlikely that human error mechanisms which could significantly affect nuclear safety risk have remained unidentified for analysis and assessment.

## 5.2. OVERVIEW AND BASIS FOR APPROACH

This section provides an overview of, and basis for, the process for identifying and assessing Type A, B and C HBSCs, including references to the sections of this sub-chapter which discuss the approach and results for each type of HBSC in more detail.

The process used to identify and assess pre- and post-fault HBSCs (i.e. Type A, B and C HBSCs) is based on a combination of OPEX, formal safety analysis and Human Factors analysis methods.

In relation to Type A HBSCs, the UK EPR PSA includes explicit modelling of human errors associated with misalignment of manual valves during maintenance performed during at-power and shutdown states. These were identified through a combination of OPEX and expert judgement. Misalignment of motor operated and solenoid valves is not explicitly modelled in the PSA as they are automatically realigned on safety demand or their misalignment is indicated by alarms in the Main Control Room. To confirm this, an assessment of design and operating features associated with the motor-operated and solenoid valves has been carried out [Ref-1].



<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 75 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

The UK EPR specific HFE programme of work included the development and implementation of an approach to identify and assess Type A pre-fault HBSCs associated with maintenance, testing and calibration activities on risk significant equipment modelled in the PSA. The approach taken is based on UK and international guidance [Ref-2] [Ref-3]. Focusing on this subset of Type A HBSCs was judged to provide the most potential to benefit nuclear safety at the GDA phase as it enabled the identification and assessment of risk significant Type A human failure events associated with planned maintenance on safety related equipment. Recommendations for control measures to reduce the risks associated with Type A human errors for safety significant equipment to ALARP were identified.

Section 5.3.1 and 5.3.2 of this sub-chapter provides a more detailed summary of the process used to identify and assess Type A HBSCs modelled in the PSA, along with the results obtained. Section 5.4.1 of this sub-chapter provides a detailed summary for the deterministic safety analysis.

Type B HBSCs (pre-fault human errors leading to an Initiating Event) were identified through a combination of formal Human Factors analysis of generic maintenance, testing and calibration tasks associated with risk significant equipment modelled in the PSA, OPEX, and studies of specific safety case topics (e.g. dropped loads, heterogeneous boron dilution faults). These three sources provide broad coverage of potential safety significant Type B human errors or violations. The consideration of the specific safety case topics enabled the identification of human failure events associated with potential low frequency events that have not occurred on existing plants, but which could have high safety significance.

The work carried out to identify Type B human errors at the generic design phase does not include a systematic examination of operations tasks to identify errors that could lead to the occurrence of latent failures or initiating events. It is judged to be difficult to carry out a systematic identification and analysis of operational Type B errors when the detailed design is not complete and there are no operational procedures available. Generic information is available but its value for this type of analysis for UK EPR is judged to be limited. At the generic design phase, use of OPEX is considered a more appropriate method to identify safety significant pre-fault errors arising from normal operations.

The assessment of Type B pre-fault HBSCs during the generic design phase included Human Factors analysis of generic maintenance, testing and calibration tasks associated with risk significant equipment modelled in the PSA. Specific Type B HBSCs modelled in the PSA were also assessed and substantiated. These consisted of errors leading to homogeneous boron dilution and uncontrolled level drop during shutdown state and failures to respond to an initial fault that does not of itself immediately lead to an initiating event (specifically related to fire or flooding).

Section 5.3.2 of this sub-chapter provides a more detailed summary of the process used to identify and assess Type B HBSCs for systems and equipment modelled in the PSA, and the results. Section 5.4.1 of this sub-chapter provides a detailed discussion for the identification and substantiation of Type B HBSCs as part of the deterministic safety analysis.

Type C (post-fault) Human Based Safety Claims have been identified and quantified (i.e. Human Error Probabilities assigned) as part of the Level 1 and 2 PSA methodology. For the deterministic case, Type C HBSCs were also identified through the deterministic safety analysis of Steam Generator Tube Rupture, and heterogeneous boron dilution, and the internal hazards analysis of internal flooding. During GDA issue resolution, a small number of manual actions related to the safety cases for the spent fuel pool and the fault studies technical area were identified. There was sufficient confidence that these actions were achievable with an adequate level of reliability, but that further substantiation would be required during the site licensing phase.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 76 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

A proportionate, risk-based approach has been applied to the scope and level of Human Factors assessment of Type C HBSCs. This is consistent with the SAPs on fault analysis [Ref-4] and with relevant international guidance [Ref-3]. A screening process, based on nuclear safety risk has been applied to identify Type C claims in the PSA for further Human Factors analysis. For the Type C HBSCs identified through the deterministic safety studies, the bounding cases, i.e. the most nuclear safety significant claims, were identified from the respective fault studies.

Risk significant Type C claims in the PSA and deterministic safety case have been qualitatively assessed using formal task analysis methodologies [Ref-5] to confirm that the actions are achievable (can be completed in the available time) and that the claimed actions can be reliably performed (i.e. to substantiate the claimed level of reliability). The task analysis approach is consistent with the principles embodied in the SAPs [Ref-4] including EHF.5 (Task Analysis) and EHF.10 (Human Reliability).

A more detailed discussion of the method to identify and substantiate Type C HBSCs and summary of the results is provided in section 5.3.3 of this sub-chapter for HBSCs in the PSA. Section 5.4.2 of this sub-chapter details the approach and results for identification and substantiation of Type C HBSCs as part of the deterministic safety analyses.

The scope and approach taken to substantiate post-fault HBSCs provides confidence that any generic Human Factors issues that should be considered in the generic design have been identified. The approach has enabled the assessment of key UK EPR design and operating concepts such as the generic design of the MCP [PICS] (see section 4.3 of this sub-chapter), the State Oriented Approach to emergency operation (see section 4.5 of this sub-chapter), and aspects of the operating team staffing concept (see section 4.4 of this sub-chapter), in relation to fault scenarios where human error would be significant to safety.

Collectively, the scope and level of assessment of HBSCs provides breadth of coverage in relation to;

- the different categories of HBSCs (Type A, B and C);
- types of Human Failure Event (human errors and violations);
- task types and characteristics (operations and maintenance tasks, MCR and local-to-plant locations, long and short duration tasks, different performance shaping factors);
- plant operating states (A, B, C, D, E and F);
- operating categories (normal, emergency and Severe Accident).

Particular focus has been paid to areas that it is considered will derive the most nuclear safety benefit from Human Factors assessment at the generic design phase. These include the assessment of risk significant post-fault claims on operator action, and the identification and analysis of potential human errors associated with maintenance, testing and calibration tasks for risk significant systems modelled in the PSA. In accordance with the ALARP principle, issues and recommendations have been identified through the Human Factors analyses of Type A, B and C HBSCs where appropriate. For some of the Type C claims, resolution of the identified issues is required to substantiate the claimed level of human reliability or achievability of the claim within the time available. The issues identified relate to aspects of the HMI, procedures and other areas (e.g. allocation of tasks to different MCR team members) and are recorded in the UK EPR HFIR. No fundamental issues with the UK EPR design or operating concept have been identified through the HF analysis of HBSCs, and it is therefore appropriate that options are evaluated and agreed during the detailed design phase.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
		PAGE : 77 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

## CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS

Identification and substantiation of HBSCs is an iterative process. The work completed during the generic design phase represents an initial identification and substantiation of HBSCs. It is based on the design and operating information available and on a number of assumptions. The future licensee is responsible for review of the completeness of HBSCs identified in the safety case, and for completing the substantiation of HBSCs as part of the future revision of the UK EPR PSA/HRA. The future licensee is also responsible for review and selection of design options to address issues identified through the analyses of HBSCs, and validation of the assumptions underpinning the analyses. Assumptions are recorded in the UK EPR GDA Human Factors Assumptions Register to facilitate this process.

### 5.3. HUMAN BASED SAFETY CLAIMS IN THE PSA

#### 5.3.1. Summary of Overall HRA Methodology

This section summarises the overall HRA methodology for the UK EPR. A more detailed discussion of the process for identification of pre- and post-fault human failure events is provided in sections 5.3.2 and 5.3.3 of this sub-chapter respectively.

HRA has been performed in the development of the PSA, taking into account the UK EPR Reference Design and addressing the UK licensing context [Ref-1] [Ref-2].

PSA and HRA studies aim to identify, model and analyse significant human failure events, including both contributors to events (pre-fault HBSCs; Type A and B), and reliance on human actions to mitigate an event (Type C HBSCs). The results from the PSA/HRA studies are incorporated into the HFE design process with the objective of ensuring that the HMI design minimises potential errors during the performance of risk significant Human Actions, supports the detection of errors, and provides opportunities to recover from errors [Ref-1] [Ref-2].

The integration of HRA with HFE helps designers to:

- give special attention on a proportionate basis to those plant scenarios where risk significant Human Actions have been identified by PSA/HRA, and;
- confirm that human-error mechanisms are addressed in the design and operating concept to minimise the likelihood of human error, and to verify that errors are detected and recoverable.
- ensure that the design is ALARP from a Human Factors perspective.

Key design principles include:

- reducing the potential for errors when performing risk significant human actions;
- making the plant less susceptible to these errors.

The human reliability analysis model used in the Level 1 PSA to assess the probability of human error is applied to a set of scenarios and accident sequences that contribute to Core Damage Frequency (see Sub-chapter 15.1).

The UK EPR PSA includes human errors associated with Type C (post-fault) Human Based Safety Claims, and human errors associated with Type A HBSCs relating to misalignment of manual valves during maintenance performed during at-power and shutdown states. Misalignment of motor operated and solenoid valves is not modelled in the PSA as noted in section 5.2 of this sub-chapter and [Ref-3]. A summary of key claims made on operator action in the UK EPR Level 1 and Level 2 PSA is provided in [Ref-4] [Ref-5].

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 78 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

Potential pre- and post-fault human errors were identified for inclusion in the PSA based on OPEX and Subject Matter Expert judgement. As the full set of Emergency Operating Procedures is currently not defined for the UK EPR, the following criteria were used to determine the post-fault human actions modelled in the PSA [Ref-4]:

- performance of irrelevant actions (aggravating errors) that have the potential for contributing to additional system failure/unavailability was not addressed at this stage;
- recovery actions described in the accident analyses of the EPR Basic Design Report are modelled in the PSA. These actions have been determined before the writing of the Emergency Operating Procedures specific to the EPR design. In order to determine those actions, typical PWR actions and operating procedures adapted to the EPR design have been used;
- recovery actions with a time window shorter than 30 minutes are not considered in the deterministic safety analysis but are modelled in the PSA if:
  - It is a back-up of an existing automatic action and
  - There are sufficiently clear indication available to the operator and
  - The time window is greater than 10 minutes.
- additional recovery actions have been identified using expert judgment of PSA and EOP experts;
- life threatening actions are not considered.

Once these actions had been selected they were assessed as part of the level 1 and level 2 PSA/HRA process, as described in the methodology described below.

The HRA approach adopted for the Level 1 PSA (see Sub-chapter 15.1) is adapted from the methodology developed by Swain in the Accident Sequence Evaluation Program (ASEP) Human Reliability Assessment Procedure [Ref-6]. Fundamentally, this approach represents a simplification of the Technique for Human Error Rate Prediction (THERP) approach developed by Swain and Guttman [Ref-7]. ASEP is a rule-based methodology which addresses both pre-accident and post-accident tasks (and hence pre-fault and post-fault Human Factor Events). For each of these event types it comprises a 'screening' HRA and a 'nominal' HRA. The screening HRA is more conservative than a nominal HRA. It has been adapted to preclude the need for the exhaustive identification and weighting of performance shaping factors demanded by the THERP methodology while still producing valid, but conservative Human Error Probability (HEP) values for input to PSAs for nuclear facilities. It employs the THERP model for modelling direct dependencies between human failure events (human errors or violations).

This approach is appropriate for derivation of human error probabilities when there is insufficient data available in relation to the task environment to comprehensively identify the Performance Shaping Factors for a task or accurately assess their cumulative effect on operator reliability. This is the current situation for the UK EPR since the Reference Design is the Flamanville 3 Initial Reference Design frozen in December 2008 before the design of the Main Control Room layout, the Human-Machine Interface, the Emergency Operating Procedures and staffing levels had been established. It should be noted that there will be differences between the final FA3 design and the UK EPR design and that future revisions to the PSA will reflect these.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 79 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

Thus the ASEP approach is considered to be appropriate for application to pre-fault and post-fault human errors at this time. Because ASEP employs more conservative assumptions about the probability of error arising from response times, recovery factors and other human performance characteristics, there is confidence that the output HEP values are conservative and do not represent an overestimation of operator reliability. It should also be noted that PSA/HRA, like other aspects of the HFE programme, is an iterative process. The PSA/HRA (including HEP values) will be revisited and updated as appropriate during the site licensing phase. The results of the task analysis described in section 5.2 of this sub-chapter provide an input to future iterations of the PSA/HRA.

ASEP employs a number of simplifying assumptions to enable the assessment of Human Error Probabilities. In addition, the PSA analysis has defined a number of assumptions about procedures, training and operating team concept to ensure the applicability of the methodology to the preliminary design phase. The lack of finalised operating procedures and operating team concept at the current stage of design, therefore leads to the key assumption of the Level 1 PSA in that the HRA is performed under the assumption that the operating procedures and guidelines will be well written and complete, as will operator training.

The Level 2 PSA (see Sub-chapter 15.4) uses an approach for evaluating HEPs for Severe Accident management strategies based on the well-known SPAR-H method [Ref-8]. The SPAR-H approach is adapted to the particularities of Severe Accident guidance (Operating Strategy for Severe Accidents), to the Severe Accident emergency organisation, and to the evaluation of positive and negative impacts that is required in the case of a Severe Accident. The Performance Shaping Factors used in the Standardised Plant Analysis Risk – Human Reliability Analysis (SPAR-H) method are consistent with those identified in recommended practices for HRA [Ref-9].

In conclusion, ASEP has been used to evaluate HEPs in the Level 1 PSA, and SPAR-H for HEPs associated with Severe Accident strategies. These methods are considered to be appropriate for the GDA phase for the reasons outlined above.

### **5.3.2. Identification and substantiation of Pre-fault HBSCs for systems and equipment modelled in the PSA (Type A and B)**

#### **5.3.2.1. Type A**

Type A errors modelled in the UK EPR PSA have been assessed using the HRA methodology described in section 5.3.1 of this sub-chapter, including quantification of human error probabilities. These potential errors relate to the misalignment of manually operated valves.

Additional studies have been carried out as part of the UK EPR specific HFE programme of work to complete the identification and assessment of Type A errors for the generic design phase. These studies were based on a pre-fault task analysis methodology developed by EDF/AREVA [Ref-1]. The methodology involved the following steps:

- Step 1: Risk based screening of the PSA [Ref-2] failure modes to identify risk significant items of equipment (regarding their post-fault duties during mitigation of accident sequences). The selection criteria for the PSA basic events was Risk Importance Factor (RIF) > 2 or Fussell-Vesely (FV) > 5E-3 with regard to CDF or LRF (as per the methodology) [Ref-1];

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 80 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

- Step 2: The risk significant items of equipment were categorised as to whether they were legacy or non-legacy [Ref-3]. Legacy equipment was defined as equipment for which there is substantive information and experience within EDF/AREVA. Non-legacy equipment was defined as equipment that is of a new design, or equipment of an existing design for which there is not substantive information or experience within EDF/AREVA;
- Step 3: Grouping of risk significant equipment by generic type [Ref-3]. Examples of equipment groupings are valves, pumps, heat exchangers, electrical systems, reactor coolant pump seals, and diesel generators. At the generic design phase, it was not appropriate to develop the pre-fault task analysis based on detailed procedures for individual items of equipment, as these procedures will be licensee specific;
- Step 4a: Identification of maintenance, testing and calibration tasks for generic equipment types using the EPRI Preventive Maintenance (PM) Basis Template Pages [Ref-3] and input from EDF and AREVA Subject Matter Experts (SMEs). This enabled the identification of generic high level maintenance, testing and calibration tasks and representative subtasks. The output is presented in [Ref-4];
- Step 4b: Where non-legacy equipment was not covered by the EPRI PM Basis [Ref-3] the maintenance, testing and calibration tasks were identified by analogy with legacy equipment and with guidance from SMEs. The output is presented in [Ref-4];
- Step 5: Task screening to identify the risk significant tasks [Ref-4]. These were the tasks where the potential consequences associated with human failure events would be the failure modes identified from the PSA in Step 1 [Ref-4]. The screening aimed to identify tasks where a human error or violation would actively introduce a latent failure into the equipment. It did not focus on potential human failure events associated with identifying existing defects with the equipment. The criteria used to screen the tasks focussed on invasiveness, the requirement for configuration changes and the need for calibration;
- Step 6: Human HAZOP of risk significant tasks. This was conducted with SMEs familiar with the maintenance and design of the equipment. The aims of the HAZOP were to:
  - identify potential errors and design induced violations that could lead to Type A and B human failure events;
  - identify, assess and substantiate the control measures in place to prevent or facilitate recovery from these human failure events in relation to the hierarchy of controls defined in [Ref-5];
  - where required, to make recommendations to improve reliability in relation to human failure events.

The use of the process described in steps 1 to 5 [Ref-1] enabled the identification of generic maintenance, testing and calibration tasks and an extensive set of subtasks, and to screen them depending on their nuclear safety significance. These safety significant tasks were the subject of the Human HAZOP analysis (step 6). The Type A analysis is independent of the reactor state in which the equipment operation is required in the PSA, and covers therefore both at-power and shutdown states.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
		PAGE : 81 / 130
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	Document ID.No. UKEPR-0002-181 Issue 06

For each safety significant task the potential human failure events (both human errors and design induced violations) that could impact on nuclear safety were identified. The tasks and potential human errors were then reviewed in the Human HAZOP analysis [Ref-5] and the hierarchy of control measures was considered. The specific equipment has not been specified or selected during the generic design phase. Therefore it was not possible to draw conclusions that the error incidence arising from the design of specific equipment and their associated maintenance, testing and calibration tasks is ALARP. However, it was possible to identify control measures that represent good practice and capture these as issues to be fed forward into subsequent stages of the design. These are discussed in the Human HAZOP analysis [Ref-5].

The analysis identified potential human errors or violations that could be eliminated by design, and provided associated recommendations to enhance nuclear safety (for example, selection of components that minimise the requirement for invasive maintenance). In other cases, potential human errors could be prevented by passive engineered measures (for example the use of interlocks) or active engineered measures (e.g. the provision of alarms). For the remaining potential human errors, administrative controls were identified as appropriate to minimise risk to ALARP. These control measures have been provided as recommendations to inform the selection of equipment in subsequent design phases that would contribute to reducing the risk from Type A human errors associated with preventive maintenance tasks such that they are ALARP. The analysis concluded that the Reference Design submitted for the generic design phase does not foreclose design options for implementing these recommendations to control the human failure events associated with pre-fault tasks.

During the Human HAZOP analysis consideration was given to design induced violations. No human failure events were identified that were specific to violations, as the ability to identify specific violations was limited because the task context cannot be defined in detail at the generic design phase (e.g. the working environment, tool design, procedures, team size, task design). However, where human failure events were identified in relation to errors, these could also arise due to violations when completing the tasks. The control measures that would eliminate, prevent or control potential errors would also address potential violations.

The identification and assessment of Type A HBSCs for the generic design phase does not include failure diagnosis and failure repair in the context of corrective maintenance. This is because it is normal practice for failure diagnosis and failure repair to use wherever possible the same processes and procedures as are used for planned maintenance. Where this is not possible then the failure and the repair will be of a nature that is non-generic and not suitable for analysis at the generic design phase of design because the tasks will be controlled through mechanisms such as risk assessments, pre-job briefings and maintenance training which will be addressed in the detailed design phase.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 82 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

### 5.3.2.2. Type B

Type B HBSCs (human errors that could lead to fault scenario initiating events modelled in the PSA) have been identified and assessed using the following methods;

- identification and analysis of potential Type B errors associated with generic maintenance, testing and calibration tasks as part of the pre-fault task analyses described in section 5.3.2.1 of this sub-chapter. As part of the Human HAZOP analysis of maintenance tasks, each task was reviewed by the SMEs to identify whether an error on that task could lead to an initiating event. This enabled the identification of tasks for which an error could result in a Type B human failure event. As these Type B human failure events represented additional potential consequences associated with an error on a task, the control measures identified to eliminate, prevent or control the Type A human failure event would also either eliminate, prevent or control the Type B human failure event. The analysis identified a number of potential Type B human failure events relating to maintenance, testing and calibration tasks associated to the following generic equipment types; valves, heat exchangers, electrical, I&C and the Standstill Seal System (SSSS). As with the Type A errors, an assessment of the adequacy of control measures was carried out. The conclusions presented in section 5.3.2.1 of this sub-chapter above also apply to the analysis of Type B errors;
- review and substantiation of Type B HBSCs associated with specific events where an explicit estimation of the human error probability has been performed to derive the initiating event frequencies in the UK EPR PSA. The specific events assessed were:
  - homogeneous boron dilution events during at-power and shutdown states;
  - uncontrolled level drop during shutdown state Cb;
  - fire in the MCR during at-power states;
  - flooding in the turbine building during at-power states;
  - flooding in the safeguard building during at-power states.

The Type B human failure events explicitly modelled in the PSA for these events consist of human errors leading to the initiating event itself (for homogeneous boron dilution and uncontrolled level drop), and failures to respond to an initial fault that does not by itself immediately lead to an initiating event (for fire in the MCR and flooding in the turbine and safeguard buildings). These Type B human failure events were reviewed and substantiated based on the following:

- evidence to support the adequacy of the OPEX process;
- justification of the initiating event frequency in the UK EPR GDA PSA; and
- evidence that learning has been applied to existing plants and carried forward to the EPR design in order to prevent the occurrence of these events.



<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 83 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

The approach and results of the review are provided in [Ref-1].

The OPEX process used by EDF [Ref-1] ensures that learning from the existing fleet and from international experience is incorporated into the generic design. The approach is consistent with international guidance on OPEX programmes, and includes processes for the collection, screening, and analysis of events, and follow-up to ensure the effectiveness of actions taken (for example, changes to design or operational practices).

The review of the Type B human failure events modelled in the UK EPR GDA PSA provides the basis for, and justification of, the initiating event frequencies that have been assigned, based on OPEX from the existing fleet and expert judgement. Where appropriate, modifications to design, operational practices and procedures have been incorporated in the generic design, based on OPEX from the existing fleet and international experience to prevent or mitigate the consequences of the events. Examples include automation of safety actions to protect against homogeneous boron dilution and provision of four redundant boron meters to detect dilution should it occur, a dedicated alarm to detect flooding in the safeguard building, and implementation of ongoing water level measurements to protect against uncontrolled level drop. It is therefore considered that the generic design includes appropriate barriers developed through OPEX to minimise the risk associated with the Type B human failure events explicitly modelled in the UK EPR GDA PSA.

### **5.3.3. Identification and Substantiation of Post-fault HBSCs (Type C)**

#### **5.3.3.1. Identification and substantiation of post-fault HBSCs (Type C) in the PSA**

Risk significant Type C claims in the PSA have been identified as part of the PSA/HRA process and qualitatively assessed using formal task analysis methodologies [Ref-1]. The purpose of the task analyses was to confirm that the claims are achievable (can be completed in the time defined in the PSA, which corresponds to the time from the occurrence of the initiating event to completion of the required actions to mitigate the fault) and that the claimed actions can be reliably performed (i.e. to substantiate the claimed level of reliability). This was achieved through application of a structured, proportionate and risk based task analytical approach. The sections below describe in more detail the approach, including the process used to screen, group and substantiate the HBSCs. A summary of the results and conclusions is also provided. Specific results and conclusions relating to design and operating concepts (e.g. HMI, staffing and procedure concept) are discussed in section 4 of this sub-chapter.

#### **5.3.3.2. Categorisation of Type C HBSCs**

All three classes of events are addressed in the HRA claims presented in the UK EPR PSA reports [Ref-1]. Categorisation criteria were used to identify the risk significant Human Based Safety Claims [Ref-1]. The derived risk categories were used to determine the degree of Human Factors assessment required to substantiate the operator claimed actions.

The method statement for the analysis of post-fault HBSCs combines the risk boundaries provided by the HRA notebook [Ref-2] and NUREG 1764 [Ref-3] to identify the most conservative model (based on FV and RIF values). This resulted in the categorisation of Type C HBSCs into low, medium and high risk significant claims, which is defined in [Ref-4].

Of the Type C HBSCs modelled in the PSA, 8 have been categorised high risk and 28 have been categorised medium risk. These claims are representative of the diversity of claims that are modelled in the UK EPR PSA, in particular regarding the following factors:

- Plant operating states: at-power state, shutdown states;

UK EPR	PRE-CONSTRUCTION SAFETY REPORT	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 84 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

- I&C availability: computerised I&C available, operation on NCSS, loss of TELEPERM XS;
- Location: Main Control Room, local-to-plant;
- Time available for action: short term, long term;
- Severity of the transient: prevention of core damage, Severe Accidents.

Although different levels of task analysis were defined in the method statement, the same level of detailed task analysis has been applied to high and most of medium claims. Of the 28 medium claims, 4 have however been analysed in a less detailed way based on probabilistic considerations [Ref-5]. The 4 medium claims relating to homogeneous boron dilution have not been assessed, this is because design options to provide protection against homogeneous boron dilution are being considered in the GDA safety case through a high level ALARP analysis, and the outcome of this process will affect the claims made in the PSA. The future licensee is responsible for the update and substantiation of HBSCs related to homogeneous boron dilution.

### 5.3.3.3. Substantiation

A task analysis methodology for post-fault (Type C) HBSCs was developed to meet the requirements of the EPR generic design phase, and Human Factors safety case approaches [Ref-1] [Ref-2]. The objectives of the task analysis were to:

- evaluate the feasibility of the operator actions associated with safety case claims, given task demands, support and conditions. This includes both Main Control Room based and field actions;
- demonstrate that it is appropriate for the safety operation to be carried out by the operator and that its automation is not necessary from a human performance perspective;
- identify any areas where, through either action or inaction, unacceptable consequences to nuclear safety may result. This includes both potential human errors and violations;
- provide a sound qualitative basis for future quantification of potential human errors. The task analyses provide an input to the subsequent quantification of HRA in the PSA during the site licensing phase;
- ensure that risks are ALARP by identifying any issues and recommendations for improvement relating to Main Control Room layout, Human-Machine Interfaces, staffing arrangements (number and allocation of responsibilities between members of the operating team), procedures, training, or other aspects of the task.

The detailed task analysis methodology was applied to all claimed operator actions categorised as high risk significance and to most of the claimed operator actions categorised as medium risk significant. Those HBSCs categorised as low risk significance were not subjected to further task analysis (over and above the analysis performed as part of the HRA process described in section 5.3.1 of this sub-chapter). The task analysis methodology is described in [Ref-1] and included the following steps;

UK EPR	PRE-CONSTRUCTION SAFETY REPORT	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 85 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

- definition of fault scenario;
- preliminary task analysis (hierarchical, tabular task analysis and time line analysis);
- OPEX Review; World Association of Nuclear Operators (WANO), Nuclear Plant Event Report (NUPER), EDF and US NRC;
- Simulator observation/Subject Matter Expert workshop/talk through using 3D CAD model;
- Finalisation of task analysis.

The analysis provided a qualitative assessment of both the achievability of the claim (can be completed in the time defined in the PSA) and the reliability of the claim (appropriateness of the level of reliability assigned in the PSA). Where dependency was claimed with other operator actions (i.e. where the likelihood of an error is dependent on other actions, behaviours, systems and operations – see Sub-chapter 15.1 for discussion of the dependency model used in the UK EPR PSA), the level of dependency was reviewed.

### 5.3.3.4. Summary of Results

This section provides a high level summary of overall conclusions from the Type C task analyses. Specific conclusions relating to the UK EPR HMI, allocation of function, operating team staffing and procedure concepts are discussed in section 4 of this sub-chapter. Conclusions and recommendations relating to specific claims are provided in the individual task analysis reports [Ref-1] to [Ref-13]. A list of the Type C HBSCs assessed during the generic design phase, including conclusions on their feasibility and assessed reliability is provided in [Ref-14].

For the majority of Type C claims it was assessed that they were achievable within the time available and that the currently assigned Human Error Probability within the PSA is appropriate. For those claims assessed to be achievable in the time available, the qualitative analysis demonstrated that there is a time margin between the assessed and claimed task duration to support error detection and recovery. The margin provides support that the current allocation of key functions to the operator is appropriate as the operator actions can be performed within the available time. The analysis also identified that the claimed operator actions are supported by procedures, the HMI and peer checking.

The claimed HEP for the majority of the claims was considered to be supported provided that the validity of the assumptions upon which the analysis/conclusions are based (e.g. task step durations) is confirmed during the detailed design phase. In some cases, conclusions regarding the achievability and claimed reliability were considered dependent on addressing specific issues relating to the HMI, procedures and other aspects identified through the analyses. These are recorded in the UK EPR GDA Human Factors Issues Register.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 86 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

For the small number of claims assessed to be unachievable within the available time, or where the currently assigned HEP was considered inappropriate, recommendations have been made. These relate to detailed design and safety analysis considerations rather than fundamental issues with the design or operating concept. They are recorded in the UK EPR GDA Human Factors Issues Register and will be addressed during the detailed design phase. Examples of issues identified through the analyses are provided in section 4 of this sub-chapter. Design issues identified through the analyses include the provision of compelling cues to the operator to perform required actions, provision of trend and rate of change information to support monitoring and early detection of changes in important plant parameters, enhancements to procedural support (clarity and inclusion of specific verification and hold point steps) and further consideration of allocation of tasks within the MCR team.

The task analyses are based on the information available at the time of the assessment, and on a number of assumptions. Assumptions have been made where design or operational information is not yet available or requires confirmation. These assumptions have been formally recorded in the GDA HF Assumptions Register and will need to be validated in the detailed design phase to fully substantiate the Type C claims. In addition, the task analyses completed during the generic design phase will need to be reviewed and updated where necessary to reflect the impacts of any changes to design, procedures and other information upon which they are based.

## **5.4. DETERMINISTIC SAFETY ANALYSIS**

Human Based Safety Claims have been identified as part of the deterministic safety analysis studies performed by the Fault Studies and Internal Hazards technical areas. Specifically this involved the identification of additional pre- and post-fault potential human errors associated with systems, equipment or scenarios compared to the HBSCs explicitly modelled in the UK EPR PSA. These deterministic HBSCs are also considered, as they could induce potential important risks of core damage or radioactive releases.

### **5.4.1. Identification and Substantiation of Pre-fault Claims (Type A and B)**

#### **5.4.1.1. Dropped Loads**

The potential for human error to contribute to a significant radiological release and/or impact the fuel assembly integrity was identified in relation to dropped loads during polar crane operation and fuel handling operations.

An analysis of the Refuelling Machine [Ref-1] and Polar Crane [Ref-2] has been carried out to identify the HBSCs associated with representative handling operations (i.e. operations that could impact the fuel assembly integrity or/and induce consequent radiological releases). For the Polar Crane, the representative cases analysed were drop of a cover slab on the reactor cavity slab or on the Reactor Pressure Vessel Head. For the Refuelling Machine, the representative case analysed was drop of a Fuel Assembly on the reactor cavity floor slab with the potential to impact nuclear safety because of damage to the reactor pool structures. These cases were selected based on the potential for nuclear safety consequences, although the subsequent internal hazards analysis (see Sub-chapter 13.2) demonstrated that these were limited.

The analysis considered both direct HBSCs (i.e. operating errors or errors when human recovery is needed) and indirect HBSCs (latent human errors when performing maintenance, calibration and testing activities). The results of the analysis will be available to be used as an input for further analysis of HBSCs associated with operations from the polar crane and refuelling machine when more information is available during the detailed design phase. This would include confirmation of direct HBSCs, identification of indirect HBSCs, substantiation of the HBSCs, and ALARP justification.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
		PAGE : 87 / 130
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	Document ID.No. UKEPR-0002-181 Issue 06

The approach is described in [Ref-3] and included the following steps:

- Identification of critical scenarios for further analysis based on a severity scale of the nuclear safety consequences of each drop;
- risk analysis based on Failure Modes and Effects Analyses (FMEAs) was performed in order to identify the direct Human Based Safety Claims, along with the lines of defence. This exercise took place in the form of multi-disciplinary workshops which included the following Subject Matter Experts; HF specialist, risk analyst, maintenance and plant outage representative, internal hazards specialist, I&C specialist, and an electrical and mechanical specialist. The THERP and ASEP human error types were used to structure the identification of potential human errors. Common cause failures were considered in the analysis.;
- a list of sub-functions and components with critical failure modes and associated relevant failure causes which can be induced by indirect human errors was produced. A list of levels of defence associated to critical failure modes whose failure can be induced by indirect human errors was also produced;
- a summary of direct HBSCs was produced, including confirmation that the generic design is acceptable and robust regarding direct human errors. For the human based lines of defence, the design adequacy was also assessed.

Basis of the risk analysis findings, the assumptions and the available input data, it was concluded that the generic design includes suitable and diverse provisions to prevent the important direct human errors. The analysis identified a number of recommendations relating to design, procedures training and other aspects. These are recorded in the UK EPR GDA Human Factors Issues Register for consideration during the detailed design phase. Assumptions made in the analysis are captured in the Human Factors Assumptions Register. The list of the Human Based Safety Claims should be confirmed, completed and substantiated during the detailed design phase, including the cases selected for analysis, the final design and the assumptions.

#### **5.4.1.2. Heterogeneous Boron Dilution**

A heterogeneous boron dilution fault can occur if a slug of a slug of un-borated water enters the primary circuit (typically through the start of a reactor coolant pump), causing a reactivity excursion. There are two distinct types of claim on operator action that are made within the defences claimed against heterogeneous boron dilution faults: explicit and implicit claims.

Implicit claims are made on operator action whenever a system / component reliability is claimed and that claimed reliability does not contain an explicit consideration of the potential contribution from operator error. For example, claiming a valve to prevent leakage is an implicit claim that if the potential human error contribution to this failure mode were to be assessed then the contribution from operator error (e.g. during maintenance, testing and calibration) would be bounded by the claimed valve reliability. Implicit claims represent Type A/B HBSCs and once identified, were assessed via the PSA methodology outlined above in section 5.3 of this sub-chapter [Ref-1]. The analysis of the generic equipment types relevant to the heterogeneous boron dilution implicit claims was carried out as part of the UK EPR specific HFE programme of work on Type A and B pre-fault HBSCs, which is summarised in section 5.3.2 of this sub-chapter. The analysis reported in section 5.3.2 of this sub-chapter covered equipment associated with heterogeneous boron dilution.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
		PAGE : 88 / 130
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	Document ID.No. UKEPR-0002-181 Issue 06

The explicit claims on operator action for heterogeneous boron dilution are defined in the Fault Schedule. They consist of operator actions and human failure events that are included in the initiating event frequencies for the bounding faults considered in the safety case. Examples of explicit claims are sampling the IRWST to ensure that it has the appropriate level of boron concentration before connection to the Residual Heat Removal System (RHRS) and response to boron concentration alarms. Explicit claims represent Type C HBSCs. A screening approach was used to identify discrete sequences requiring HF analysis.

Event sequences selected for assessment were analysed using the Type C PSA methodology [Ref-2] outlined in section 5.3.3 of this sub-chapter. The objectives were to evaluate the feasibility and assessed reliability of claimed actions associated with the bounding sequences claimed in the safety case, including the suitability of the currently claimed protection for mitigating the risks associated with heterogeneous boron dilution.

It was concluded [Ref-3] that the heterogeneous boron dilution fault scenarios have multiple protection features, most including combinations of design features, active and passive engineered safeguards and administrative controls within both the maintenance and operational domains. The identified claimed prevention and mitigation actions were assessed to be feasible, although in some cases specific design and procedural enhancements are needed in order to substantiate the claimed human error probabilities, and to ensure that the risks associated with heterogeneous boron dilution are ALARP. These are detailed design considerations and are included in the UK EPR GDA Human Factors Issues Register.

A revised overall safety case for heterogeneous boron dilution has been produced, which is supported by a detailed ALARP assessment (see section 7 of PCSR Sub-chapter 16.4). This includes a design change to provide an interlock that prevents start up of the No. 1 Reactor Coolant Pump until the RCV [CVCS] letdown has run for a sufficient period of time to ensure clearance of any un-borated slugs. The interlock provides a back-up to operator actions to run the letdown for a sufficient period to clear any slugs of water. It therefore provides an additional defence against a wide range of heterogeneous boron dilution event sequences, over and above the controls previously identified through the HF and other safety assessments conducted. Operator actions associated with running the letdown should be assessed during the detailed design phase when sufficient information is available.

#### **5.4.2. Identification and Substantiation of Post-Fault Claims (Type C)**

Type C HBSCs have been identified through the safety analyses performed by the Fault Studies technical area. These relate to SGTR scenarios. HBSCs relating to post-fault operator actions in response to flooding have been identified through the internal hazards safety studies. SGTR and internal flooding HBSCs are discussed in sections 5.4.2.1 and 5.4.2.2 of this sub-chapter. It should be noted that SGTR claims are also included in the UK EPR PSA, and have been assessed using the task analysis methodology described in section 5.3.3 of this sub-chapter.

##### **5.4.2.1. Steam Generator Tube Rupture**

A SGTR accident means that there is damage of one or several tubes in a SG and that water from the primary circuit, the RCP [RCS], leaks into the secondary system. The water in the primary circuit can be radioactive and there is a risk of contamination to the environment. Claims on operator action in the event of SGTR are made in the design basis safety case [Ref-1]. These include manually tripping the reactor or checking automatic reactor trip and SG isolation, both within 50 minutes of the initiating event. Isolation of the ruptured SG includes local-to-plant actions.

Human Factors analysis of Steam Generator Tube Rupture has been carried out in accordance with the defined methodology for analysis of Type C task analysis claims described in section 5.3.3 of this sub-chapter.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 89 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

The analysis [Ref-2] concluded that it is not possible to perform all the required tasks (Reactor Trip and Steam Generator isolation) within the 50 minutes claimed in the safety case. An ALARP Fault Studies analysis shows that as long as the operator has performed the load reduction and reactor trip within the 50 minute period, there are very low radiological consequences arising from the failure to complete the remaining manual actions. This is because the plant condition will reach automatic protection signals that will result in automatic isolation of the Steam Generator [Ref-3].

A number of issues and associated improvements were identified through the task analysis to improve the feasibility and reliability of claimed operator actions. Improvements were identified to improve navigation through the procedures, the quality of cues and indications as provided by the HMI and the task step sequences (i.e. whether the load reduction and SG isolation tasks can be performed earlier). These issues have been formally recorded in the UK EPR GDA Human Factors Issues Register.

#### **5.4.2.2. Internal flooding**

Sub-chapter 13.2 covers the identification and analysis of internal hazards, including internal flooding. The consequence of internal flooding within the classified buildings of the Nuclear Island has been evaluated. In most cases, the flooding initiators have a limited upstream volume and the designed hazard barriers are sufficient to retain the bounding leak volume within the relevant building's safety division. However, some unmitigated flooding initiators have an unlimited upstream volume which could exceed the building's water retention capability and thus ingress into another safety division overcoming the segregation of safety classified equipment [Ref-1].

Human Factors analysis has been carried out of both the generic operator response to a leak and analysis of an appropriate sample of internal flooding scenarios. The objectives of the analysis were to substantiate the claims on the operator contained within the internal flooding safety case, provide an input to the optioneering being performed as part of the GDA ALARP analysis for mitigation of internal flooding scenarios, and support the assessment of the achievability of any HBSCs that are part of the final safety justification for internal flooding.

The selection of scenarios was based on the following criteria [Ref-2], which were judged to define demanding operator response:

- the isolation procedure (including secondary isolation to mitigate a single isolation failure) requires more than two valve operations; and;
- the isolation must be completed within 24 hours.

Five scenarios met the criteria specified above for HF analysis. The analyses were carried out in accordance with the Type C task analysis methodology described in section 5.3.3 of this sub-chapter.

The selection of the initial set of analyses was based on the initial failure criterion for classified medium energy pipework that was applied for FA3. Subsequently a final internal flooding safety case [Ref-3] that included consequence analysis of a limited number of representative cases, based on Double Ended Guillotine Break (DEGB) of classified medium energy pipework was developed. Further HF task analysis of two remote manual actions, required to be performed by the operating team, was carried out to provide necessary support to the internal flooding safety case. Both the original and the further HF analyses are reported in [Ref-2].

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 90 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

The analysis of the initial set of scenarios concluded that the leak isolation procedures claimed for three of the five scenarios analysed are achievable, with a significant margin, within the available time and the valves required for operation are accessible. The assessed task duration for completing the leak isolations procedures claimed for two of the scenarios exceeds the times that are available. These scenarios have the shortest available times of those analysed. The further internal flooding analyses performed to consider DEGB breaks of classified medium energy pipework have resulted in recommendations for design modifications that have removed the requirement for these two actions.

The analysis of the two DEGB scenarios concluded that for one of the scenarios, the assessed task duration is the same as the available grace time. For the other scenario the assessed time was less than the available time but the small margin provided limited opportunity for error prevention and recovery. An ALARP analysis of the option to automate these actions, performed as part of the internal hazards analysis [Ref-3], concluded that the information available during the GDA phase was not sufficient to determine whether automation of these operator actions was ALARP. Further consideration of this aspect will therefore be needed during the detailed design phase.

Issues and recommendations identified through the HF analyses of the internal flooding scenarios are captured in the UK EPR GDA Human Factors Issues Register for consideration during the detailed design phase.

## 6. HUMAN FACTORS PROCESS ASSURANCE

This describes the HFE organisation and programme management processes for the FA3 Initial Reference Design HFE programme, and for UK EPR specific HF activities. This includes:

- roles, responsibilities and interfaces with other disciplines (section 6.1 of this sub-chapter);
- competence assurance (section 6.2 of this sub-chapter);
- processes to oversee and assure the quality of sub-contracted HF work (section 6.3 of this sub-chapter);
- processes to ensure that HF considerations are integrated into design, including HF issues management and documentation (section 6.4 of this sub-chapter);
- design change control processes (section 6.5 of this sub-chapter).

The overall process for integrating HF into the design of the FA3 Initial Reference Design and UK EPR specific HF studies are described in section 3 of this sub-chapter.

### 6.1. ROLES, RESPONSIBILITIES AND INTERFACES

A description of the project organisation and responsibilities for the generic design phase is provided in Sub-chapter 21.1. Sections 6.1.1 and 6.1.2 of this sub-chapter summarise responsibilities for the FA3 Initial Reference Design HFE programme and UK EPR specific HF activities. Responsibilities for the FA3 Initial Reference Design are included because the HF element of the safety case for the generic design is based on the results of the FA3 HFE programme and UK EPR specific HF activities (see section 3 of this sub-chapter).



<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 91 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

### **6.1.1. FA3 Initial Reference Design**

To ensure that the HFE programme for the FA3 Initial Reference Design was effectively implemented, a multi-disciplinary EDF team was established. The team included Human Factors Specialists, Design Engineers, Operators, Technicians and Nuclear Operation Department's Representatives. The roles and responsibilities of these groups are described below:

#### **6.1.1.1. Human Factors Specialists**

A Human Factors Coordinator within the Project Service of the Nuclear Equipment Department is responsible for the FA3 HFE programme and for its coordination. The HF Coordinator is supported by HF specialists with additional support from contractors where necessary.

The HF Coordinator is attached to the Technical Director of the EPR Project, in the Nuclear Engineering Department. This organisation enables the HF Coordinator to:

- benefit from all the technical and managerial information on the EPR Project, thus enhancing the ability to contribute, when required, to the reviews and forums where design choices are made;
- identify as required the need for HF studies and assess the potential impacts of design choices on human performance;
- work directly with the design teams in an iterative manner to integrate:
  - relevant OPEX from existing plants;
  - the HF perspective as regards design studies and choices which support the needs of future users of the plant. This involves review of the design studies carried out by the Design Engineers;
  - Human Factors standards and requirements applicable to the design phase,
  - studies evaluating the design choices, particularly by using tests involving representatives of the future users;
- co-ordinate the activities of other HF specialists from different groups including the Nuclear Engineering Department, Research and Development Department, Nuclear Operation Department, Health Service, external Human Factors specialists.

#### **6.1.1.2. Design Engineers**

Design Engineers from the various Engineering Business Units (e.g. I&C, electrical, mechanical, civil) are stakeholders in the HFE programme. Achieving the design-programme objectives necessarily requires considering HF as an integral part of their design activities. The following means are used within the FA3 EPR Project organisation to integrate HF issues into the Design Engineers' activities:

- supporting documentation for the design must enable HF requirements and considerations to be integrated into the design choices. The HF Coordinator is involved, as appropriate, in drafting documents that define the engineering activity (Design Quality Plans) and that describe the methods to use (Engineering Rules). In this way, the engineering documents relating to automation, system design and system management take proper account of HF;

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 92 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

- Engineers and Human Factors specialists collaborate on particular pieces of work or studies that form an integral part of the design studies. Such work includes, for example, the design and evaluation of the operational interfaces, and the studies for maintenance activities, carried out in collaboration with experts from civil engineering disciplines.

#### **6.1.1.3. Operators and Nuclear Operation Department's Representatives**

For the FA3 EPR Project, EDF Nuclear Operation Department has acted as a stakeholder via a team seconded to EDF Nuclear Engineering Department. The team includes a number of specialists in maintenance, operational management, radiation protection and general operations. The members form a point of contact between the plant operators and Nuclear Operation Department's corporate level and design services.

The Operator's Representatives, like the Design Engineers, take part in the HFE programme activities to:

- ensure that the future operator's views and requirements are taken into account;
- provide the EPR with the benefit of their extensive experience of operating nuclear plants;
- use their knowledge of plant operation to assist the HFE studies carried out to define the requirements of future users, and to consult with operators in existing plants;
- define the programme priorities.

In addition to the seconded team described above, operations and maintenance staff from the existing fleet participate in the HF evaluation process. They provide comments on positive and negative aspects of the current designs, give their opinion on options and, if necessary, supplement the design requirements.

The participation of existing operations and maintenance representatives in the design process in general, and in the HFE programme in particular, is an important factor in incorporating Human Factors into the FA3 EPR design. This approach is in accordance with ISO 13407 [Ref-1].

Note that a discussion of the FA3 Initial Reference Design PSA/HRA responsibilities is not provided, since a specific PSA and HRA has been produced for the UK EPR.

#### **6.1.2. UK EPR Specific Roles, Responsibilities and Interfaces**

Roles, responsibilities and interfaces for UK EPR specific HF analysis and inputs are described in sections 6.1.2.1 to 6.1.2.7 of this sub-chapter and in [Ref-1].

Defining and setting up the HF team responsible for performing the tasks that are required for future phases of the project is the responsibility of the UK licensee, as is the definition of the future HFE organisation for the operational phase.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 93 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

#### **6.1.2.1. Human Factors Technical Lead**

The EDF Human Factors Lead is responsible for co-ordinating and acting as the Intelligent Customer for work performed in connection with UK EPR specific HF activities. This includes the following specific responsibilities:

- specifying and overseeing the work performed by HF specialists, including HF contractors;
- participating in HF analyses and reviews;
- ensuring technical verification of HF deliverables by the appropriate experts;
- coordinating HF input to the specifications for UK EPR design modifications;
- interfacing with other technical disciplines, and the FA3 HF Specialists, to ensure appropriate inputs to, and integration of HF activities.

#### **6.1.2.2. Human Factors Co-applicant Technical Correspondent**

The AREVA Human Factors Co-applicant Technical Correspondent is the counterpart to the Technical Lead in the co-applicant organisation. The Co-applicant Technical Correspondent has, jointly with the Technical Lead, overall technical and coordination responsibility for the HF activities defined in section 6.1.2.1 of this sub-chapter.

#### **6.1.2.3. Human Factors Specialists**

The UK EPR HF analyses are carried out by Human Factors Specialists from suppliers of nuclear engineering and safety case services. They are responsible for:

- developing methods and approaches for HF analyses which meet UK and international good practice;
- carrying out analysis of pre- and post-fault Human Based Safety Claims as part of an EDF/AREVA multi-disciplinary team (section 5 of this sub-chapter provides further details);
- identifying and recording HF issues and assumptions so they can be addressed and managed.

#### **6.1.2.4. Operations and Maintenance Specialists**

EDF/AREVA SMEs are responsible for providing support and information to the HF Specialists on the design, operation and maintenance of the UK-EPR as part of the HF analysis data collection and verification process. As UK EPR operations and maintenance staff are not available at this point in the project, SMEs are identified as EDF/AREVA engineers, operations or maintenance Subject Matter Experts with relevant EPR experience.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 94 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

#### **6.1.2.5. PSA specialists**

A specific PSA/HRA has been developed for the UK EPR. PSA/HRA specialists are responsible for the identification, modelling and analysis of human actions in the PSA, including their quantification. Where risk significant Human Actions are determined, they are incorporated into the HFE design process with the objective of ensuring that the design minimises potential errors during the performance of risk significant Human Actions, supports the detection of errors, and provides opportunities to recover from errors [Ref-1] and [Ref-2]. The integration of HRA with HFE helps designers to:

- give special attention on a proportionate basis to those plant scenarios where risk significant Human Actions have been identified by PSA/HRA, and;
- confirm that human-error mechanisms are addressed in the design of the HMI to minimise the likelihood of human error, and to verify that errors are detected and recoverable.

Pre- and post-fault claims modelled in the UK EPR PSA have been substantiated through HF analysis, using a proportionate, risk based approach.

In relation to post-fault claims, PSA specialists are responsible for providing information to the HF specialists on claims to be assessed through task analysis. PSA specialists work with the HF specialists to develop the description of the scenario to be analysed, and provide information on the safety case, design and plant operation to support the task analysis data collection and verification process. For pre-fault claims the PSA specialists are responsible for providing information on failure modes and risk significance of plant systems and components.

#### **6.1.2.6. Fault Studies Specialists**

Fault Studies specialists are responsible for working with the HF specialists to identify pre-fault and post-fault Human Based Safety Claims arising from the fault studies. The key areas considered in the HF pre-construction safety case are heterogeneous boron dilution and single tube steam generator tube rupture, based on nuclear safety risks. This includes development and implementation of a methodology for the identification and analysis of Human Based Safety Claims, to the extent possible at the current stage of design.

#### **6.1.2.7. Internal Hazards Specialists**

Internal Hazards specialists are responsible for working with the HF specialists to identify pre-fault and post-fault Human Based Safety Claims arising from the deterministic safety analysis. The key areas considered in the HF pre-construction safety case are dropped loads and internal flooding, based on nuclear safety risks. This includes development and implementation of a risk analysis methodology for the identification and analysis of Human Based Safety Claims, to the extent possible at the current stage of design.

### **6.2. COMPETENCE ASSURANCE**

Sub-chapter 21.2 summarises the approach to ensure that personnel involved in the project activities are suitably qualified and experienced for the tasks assigned to them.

#### **6.2.1. FA3 Initial Reference Design**

Competence assurance for EDF HF specialists is achieved through initial recruitment processes and specific training (on the job and formal courses) on nuclear power plant design, nuclear safety and other relevant topics.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER: 18.1
		PAGE : 95 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

A training course in HF has been developed by EDF for Design Engineers working on the FA3 Initial Reference Design. The course lasts two days and is centred on design ergonomics and HFE in the design phase. It provides the Design Engineers with some basic knowledge of the discipline, enables them to understand the HF approach, and identify areas that require consideration of HF. A one-day HF training course for managers has also been developed, using a condensed form of the Design Engineer HF training material.

### **6.2.2. UK EPR specific HF studies**

The competencies required by suppliers to perform Human Factors work in support of the design are defined by invitation to tender documents. Selection of suppliers includes a review of organisational and individual competencies required for the type and scope of services to be supplied.

The UK EPR specific HF studies have been carried out by Human Factors specialists from recognised suppliers of nuclear safety case services.

## **6.3. OVERSIGHT OF SUB-CONTRACTORS**

### **6.3.1. FA3 Initial Reference Design Work**

A process exists for the monitoring and oversight of contractors carrying out layout studies and design work [Ref-1]. This process defines how monitoring should be conducted and who should be involved. A programme has been developed for monitoring the two principal EPR layout design contractors: Sofinel and AREVA. The contract monitoring documents specific to layout design are included in the generic process for the monitoring of suppliers.

### **6.3.2. UK EPR specific HF Studies**

The EDF HF Lead is the Intelligent Customer for HF work performed by suppliers. The technical quality of the work is ensured by;

- appropriate specification of work;
- provision of information and resources necessary to perform the work (e.g. access to the simulator, operations representatives, documentation);
- close interaction with the supplier throughout the work (including participation in meetings and simulator observations), and;
- technical review of deliverables by the appropriate experts.

The process for EDF/A review of HF deliverables produced by suppliers is described in [Ref-1].

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
		PAGE : 96 / 130
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	Document ID.No. UKEPR-0002-181 Issue 06

## **6.4. HFE PROCESSES AND DOCUMENTATION**

### **6.4.1. FA3 Initial Reference Design**

#### **6.4.1.1. Design Quality Plan**

The Human Factors programme for the FA3 Initial Reference Design is described in a Design Quality Plan (DQP). This is summarised in section 3 of this sub-chapter and [Ref-1]. The Human Factors DQP describes the scope and approach to integrate Human Factors into design and review activities. It specifies the application of the Human Factors design programme during the different phases of the EPR design process. It also details the specific role of the Human Factors coordinator and other EPR project team members in the design process.

The results of the HFE programme are recorded in HF reports and design documents. These include documents presenting methods and results of HF studies carried out as part of the review of OPEX, analysis of operator tasks, team organisation studies, verification and validation of the design.

#### **6.4.1.2. OPEX**

HF studies to identify strengths and potential improvements to design and operating concepts have been carried out as part of the FA3 HFE programme. The outputs from these studies are recorded in HF reports and design specifications for EPR HMI, I&C, buildings, systems, equipment and components (see sections 3 and 6.4.1.3 of this sub-chapter).

#### **6.4.1.3. Design Specifications**

HF specialists were involved in working groups to define the principles of computerised operation, emergency operation, normal operation and automation. The outputs from the working groups provided an input to the development of the design specifications.

The specifications for EPR I&C, HMI, buildings, systems, equipment and components include requirements from a number of sources including regulatory, industry, and internal requirements. Operations, maintenance, construction and HF requirements are included in the specifications [Ref-1] to [Ref-5], along with requirements based on OPEX from the EDF fleet. Specifications are issued under invitation to tender and associated contract documents, which include HF requirements as appropriate.

#### **6.4.1.4. HF Evaluation and Review of Design**

Section 3 of this sub-chapter describes the iterative process used for HF evaluation and review of the FA3 Initial Reference Design. The HF Design Quality Plan states that there will be HF participation in the design evaluation reviews that are specified in the Installation Design Quality Plan. An input to this design process has been provided by a Human Factors specialist.

FA3 Human Factors specialists are involved in the review of responses to invitations to tender for aspects such as the MCR HMI and the layout of safety-related buildings. Operation Department representatives also review the design specifications.

The HFE programme for evaluation of EPR operation before the first fuel loading is defined in [Ref-1]. This includes the Verification and Validation process for the MCR [Ref-1] [Ref-2].

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER: 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 97 / 130
		Document ID.No. UKEPR-0002-181 Issue 06

Processes also exist to obtain multi-disciplinary inputs on different design topics throughout the FA3 design process. These include:

- permanent technical committees, design committees and periodic technical review meetings on topics such as environmental protection, outages, radiation protection. Human Factors specialists and contractors participate in these committees and review meetings where appropriate;
- the building review process: to study the layout of rooms and to verify accessibility to and maintainability of equipment, consistent with installation and layout rules (see section 3 of this sub-chapter for more details).

#### **6.4.1.5. HF Issues and Assumptions Management**

The results of the FA3 HFE programme, including issues, any assumptions and recommendations, are documented in technical reports and presented in multi-disciplinary technical reviews.

The design options that are the result of the HFE programme are presented and analysed in these reviews. The reviews make informed recommendations to be taken forward in the EPR design process. The technical reviews are chaired by and composed of senior managers. Significant issues or conflicting requirements are taken forward to a management committee for resolution.

#### **6.4.2. UK EPR Specific HF studies**

##### **6.4.2.1. HF Documentation**

UK EPR specific analyses are documented in technical reports, which are produced, verified and issued in accordance with project processes.

##### **6.4.2.2. HF Issues and Assumptions Management**

Human Factors issues arising from UK EPR specific analyses are recorded in HF and other relevant project reports. Issues and recommendations relating to HMI, procedures, operating team concept and other aspects are recorded, tracked and addressed through the UK EPR GDA Human Factors Issues Register [Ref-1]. A UK EPR GDA Human Factors Assumptions Register has also been developed to capture assumptions made in the analyses to enable these to be verified and validated by the future licensee [Ref-1]. The UK EPR GDA Human Factors Issues and Assumptions Register processes are governed by a procedure [Ref-1]. The objectives are to:

- identify HF issues and assumptions;
- propose recommendations to address identified issues for consideration during the detailed design phase, where appropriate;
- ensure effective handover and tracking of issues and assumptions identified during the GDA phase.

During the GDA phase, issues and assumptions are categorised in relation to the HFE programme area (e.g. procedures, HMI design, team organisation). An initial sentencing of issues is carried out. Within the frame of GDA, the scope of sentencing includes ensuring that there is a common understanding of the issue among the main disciplines responsible for their resolution.

UK EPR	PRE-CONSTRUCTION SAFETY REPORT	SUB-CHAPTER: 18.1
		PAGE : 98 / 130
		Document ID.No. UKEPR-0002-181 Issue 06
CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS		

### 6.5. DESIGN CHANGE CONTROL PROCESSES

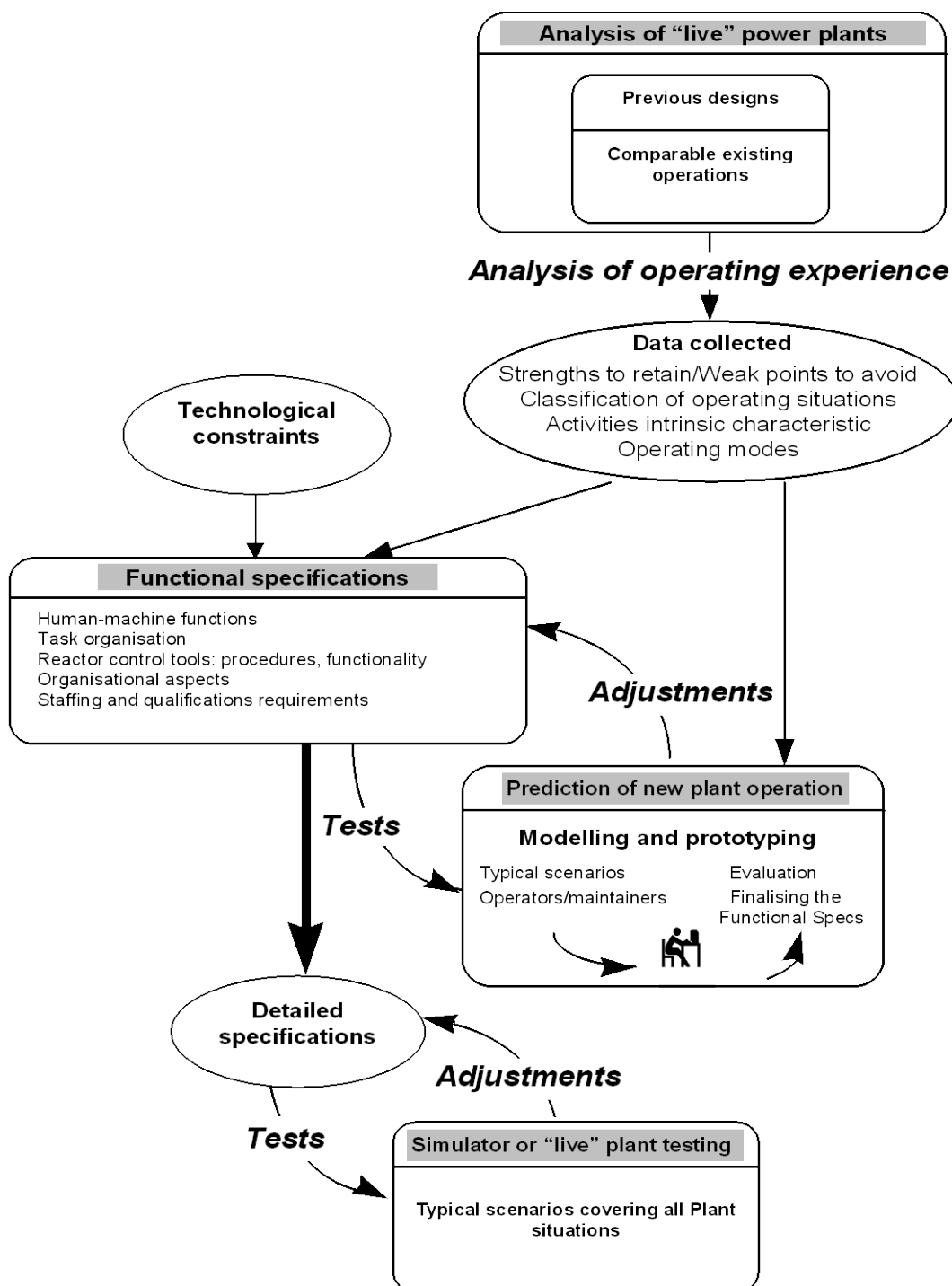
The Reference Design configuration is defined in [Ref-1]. This reference provides the baseline for the UK EPR generic design assessment change management process.

Proposed design changes are governed by the process described in [Ref-2], which is summarised in Sub-chapter 21.2. This includes a screening process to identify potentially impacted technical topics and associated documentation, including Human Factors.



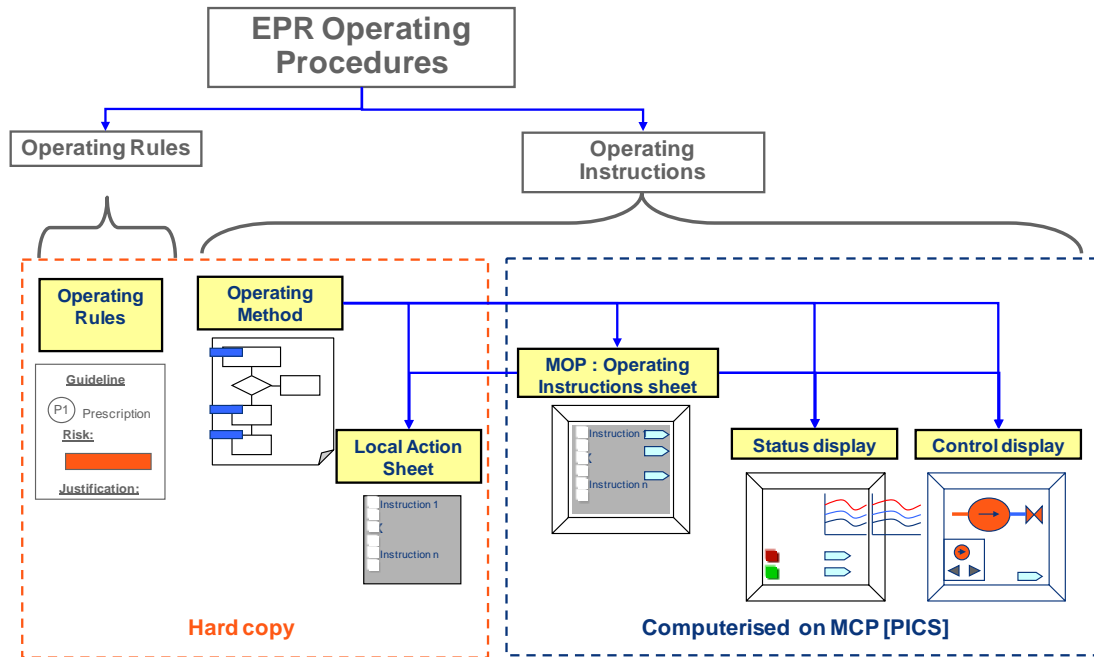
## SUB-CHAPTER 18.1 - FIGURE 1

## Human Factors Engineering programme iterative approach



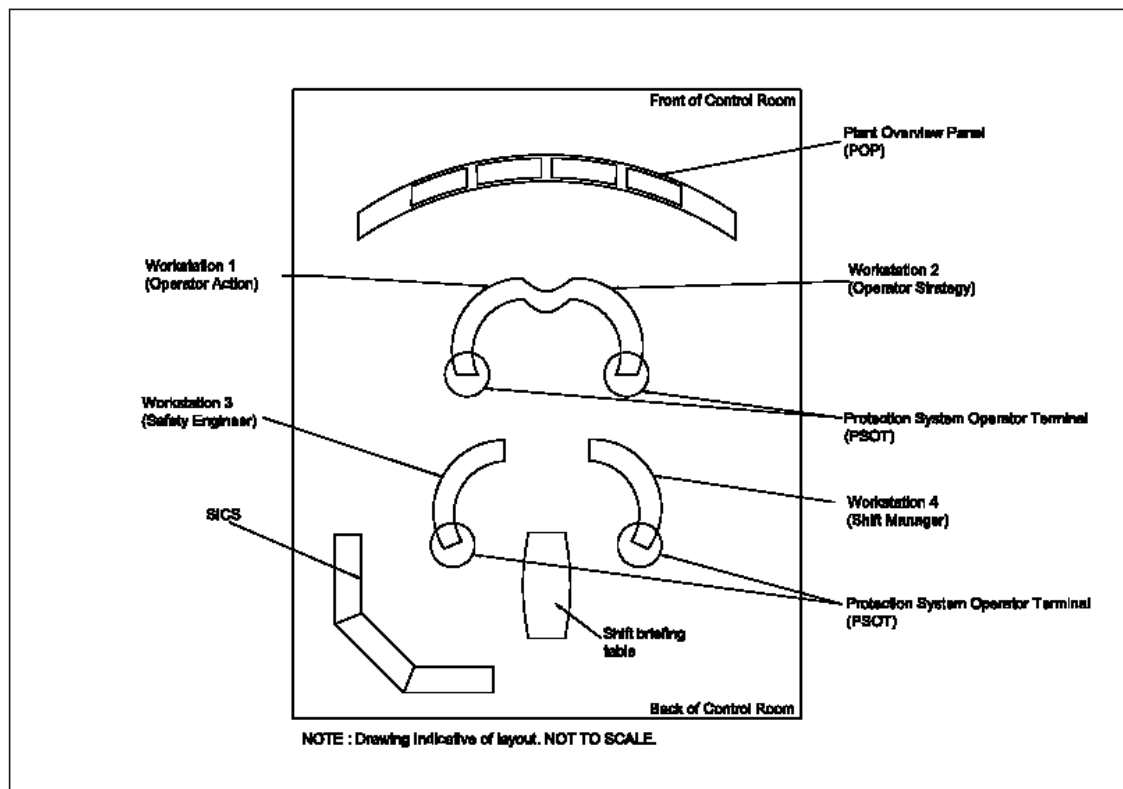
## SUB-CHAPTER 18.1 - FIGURE 2

### Indication of Operating Procedures



## SUB-CHAPTER 18.1 - FIGURE 3

## MCR Indicative Layout



<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 102 /130
		Document ID.No. UKEPR-0002-181 Issue 06

## SUB-CHAPTER 18.1 – REFERENCES

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

### 1. SAFETY REQUIREMENTS

#### 1.1. REGULATORY FRAMEWORK, EXPECTATIONS AND STANDARDS

**[Ref-1]** Safety Assessment Principles for Nuclear Facilities. UK Health and Safety Executive (HSE). 2006 Edition Revision 1. January 2008. (E)

**[Ref-2]** Human Factors Integration. T/AST/058. Issue 1. UK Health and Safety Executive (HSE). September 2010. (E)

**[Ref-3]** Management of Health and Safety at Work Regulations 1999. ISBN 0-11-085625-2. The Stationery Office Ltd. 1999. (E)

**[Ref-4]** The Ionising Radiations Regulations 1999. Statutory Instrument 1999 No. 3232. ISBN 0 11-085614-7. The Stationery Office Ltd. (E)

**[Ref-5]** International Standards, Guidelines and Technical Guidelines:

##### International Organisation for Standardisation (ISO)

- ISO 9241-210: Ergonomics of Human-System Interaction - Part 210: Human-Centred Design for interactive Systems. 2010. (E)
- ISO 11064: Ergonomic design of control centres. 2008. (E)
- ISO 9241: Ergonomics of human system interaction. 2002. (E)
- ISO 80416: Basic principles for graphical symbols for use on equipment. 2005. (E)
- ISO 7000: Graphical for use on equipment. 2004. (E)
- ISO 14617: Graphical symbols for diagrams. 2004. (E)
- ISO 13406: Ergonomic requirements for work on flat panel display screens. (E)
- ISO 15534: Ergonomic design for the safety of machinery. 2000. (E)
- ISO 14738: Safety of machinery – anthropometric requirements for the design of workstations at machinery. 2002. (E)
- ISO 6385: Ergonomics principles in the design of work systems. 1990. (E)

##### Nuclear Regulatory Commission (NRC)

- NUREG-0700: Human-System Interface Design Review Guidelines. Revision 2. 2002. (E)

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 103 /130
		Document ID.No. UKEPR-0002-181 Issue 06

- NUREG-0711: Human Factors Engineering Program Review Model. Revision 2. February 2004. (E)
- NUREG-0800 Chapter 18. Human Factors Engineering. Revision 2. 2004. (E)
- NUREG/CR-6633: Advanced Information Systems: Technical Basis and Human Factors Review Guidance. 2000. (E)
- NUREG/CR-6634: Computer-Based Procedure Systems: Technical Basis and Human Factors Review Guidance. 2000. (E)
- NUREG/CR-6635: Soft Controls: Technical Basis and Human Factors Review Guidance. 2000. (E)
- NRC NUREG-1764: Guidance for the Review of Changes to Human Actions. 2004. (E)

International Electrotechnical Commission (IEC)

- IEC 80416: Basic principles for graphical symbols for use on equipment. 2002. (E)
- IEC 61839: Nuclear Power Plants - Design of control rooms - Functional analysis and assignment. November 2000. (E)
- IEC 60073: Basic and safety principles for man-machine interfaces, marking and identification. 2002. (E)
- IEC 60447: Man-machine interface – actuating principles. 2004. (E)
- IEC 60960: Functional design criteria for SPDS. 1988. (E)
- IEC 60964: Design for control rooms of nuclear power plants. (E)
- IEC 61227: NPPs – Control rooms – Operator controls. 2008. (E)
- IEC 61771: NPPs – MCR – Design verification and validation. 1995. (E)
- IEC 61772: NPPs – MCR – Application of visual display units. 1995. (E)
- IEC 62241: NPPs – MCR – Alarm functions and presentation. 2004. (E)

Electric Power Research Institute (EPRI)

- EPRI: Human Factors Guidance for Control Room and Digital Human-System Interface. Design and Modification. 2005. (E)

Institute of Electrical and Electronic Engineers (IEEE)

- IEEE 1023: IEEE. Guide for Application of Human Factors Engineering to Systems, Equipment and Facilities of Nuclear Power Generating Systems. IEEE-1023-1988. (E)

French norms (NF)

- NF EN 897-2: Safety of machinery – Ergonomics requirements for design for means of signalling and components. (E)

UK EPR	PRE-CONSTRUCTION SAFETY REPORT	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 104 /130
		Document ID.No. UKEPR-0002-181 Issue 06

- NF D 62-042: Office furniture. Tables and desk. General characteristics. Tests and requirements.
- NF D 62-041: Office furniture. Furniture storage. General characteristics. Testing and specifications.
- NF EN 527-1, NF EN 527-3: Work tables and desks.
- NF EN 1021 parts 1 and 2: Assessment of the Ignitability of Upholstered Furniture.
- NF EN 1335-1, NF EN 1335-2 and NF EN 1335-3: Office work seating.
- NF EN 13761: Visitors seating.
- NF D 65-760: Rectangular locked metal cabinets.
- AFNOR NF X35-102: Ergonomic design for the workspace in office.

Proprietary procedures:

ENG are guidebooks for design engineer’s use. The main aim of these guidebooks is to ensure consistency and homogeneity between the various products designed.

- ENG 2-21: Degree of automation for plant systems. ECEF021855 Revision B1. EDF. May 2006. (E)
- ENG 2-31: Principles of design of synthesis information. ECEF040244 Revision D1. EDF. January 2008. (E)
- ENG 2-33: Specifications regarding the alarms. ECEF040683 Revision C1. EDF. August 2008. (E)
- ENG 2-34: Operating display format specification. ECEF040974 Revision B1. EDF. June 2006. (E)
- ENG 3-37: Design rules for operating instruction (MOP). ECEF061119 Revision A1. EDF. January 2007. (E)
- ENG 3-03 EPR Plant System Specification - Contents and Updates. ECEF050611 Revision A1. EDF. December 2005. (E)
- ENG 3-40: Content and structure of emergency operating procedures instructions. ECEF061275 Revision A1. EDF. July 2009. (E)

ECEF061275 Revision A1 is the English translation of ECEF061275 Revision A.

- Writing guide for EPR system specifications.ECEMC0000059 Revision A1. EDF. February 2010. (E)

**[Ref-6]** IAEA GS-R-1: Safety Requirements: Legal and Governmental Infrastructure for Nuclear, Radiation, Radioactive Waste and Transport Safety. (E)

**[Ref-7]** Western European Nuclear Regulators’ Association: WENRA Reactor Safety Reference Levels. 2008. (E)

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 105 /130
		Document ID.No. UKEPR-0002-181 Issue 06

**[Ref-8]** IAEA - NS-G-1.2. Safety Assessment and Verification for Nuclear Power Plants. IAEA. 2005. (E)

**1.1.2. International Standards, Guidelines and Technical Guidelines**

**[Ref-1]** International Standard Guidelines and Technical Guidelines:

International Organisation for Standardisation (ISO)

- ISO 9241-210: Ergonomics of Human-System Interaction - Part 210: Human-Centred Design for interactive Systems. 2010. (E)
- ISO 11064: Ergonomic design of control centres. 2008. (E)
- ISO 9241: Ergonomics of human system interaction. 2002. (E)
- ISO 80416: Basic principles for graphical symbols for use on equipment. 2005. (E)
- ISO 7000: Graphical for use on equipment. 2004. (E)
- ISO 14617: Graphical symbols for diagrams. 2004. (E)
- ISO 13406: Ergonomic requirements for work on flat panel display screens. (E)
- ISO 15534: Ergonomic design for the safety of machinery. 2000. (E)
- ISO 14738: Safety of machinery – anthropometric requirements for the design of workstations at machinery. 2002. (E)
- ISO 6385: Ergonomics principles in the design of work systems. 1990. (E)

Nuclear Regulatory Commission (NRC)

- NUREG-0700: Human-System Interface Design Review Guidelines. Revision 2. 2002. (E)
- NUREG-0711: Human Factors Engineering Program Review Model. Revision 2. February 2004. (E)
- NUREG-0800 Chapter 18. Human Factors Engineering. Revision 2. 2004. (E)
- NUREG/CR-6633: Advanced Information Systems: Technical Basis and Human Factors Review Guidance. 2000. (E)
- NUREG/CR-6634: Computer-Based Procedure Systems: Technical Basis and Human Factors Review Guidance. 2000. (E)
- NUREG/CR-6635: Soft Controls: Technical Basis and Human Factors Review Guidance. 2000. (E)
- NRC NUREG-1764: Guidance for the Review of Changes to Human Actions. 2004. (E)

International Electrotechnical Commission (IEC)

- IEC 80416: Basic principles for graphical symbols for use on equipment. 2002. (E)

UK EPR	PRE-CONSTRUCTION SAFETY REPORT	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 106 /130
		Document ID.No. UKEPR-0002-181 Issue 06

- IEC 61839: Nuclear Power Plants - Design of control rooms - Functional analysis and assignment. November 2000. (E)
- IEC 60073: Basic and safety principles for man-machine interfaces, marking and identification. 2002. (E)
- IEC 60447: Man-machine interface – actuating principles. 2004. (E)
- IEC 60960: Functional design criteria for SPDS. 1988. (E)
- IEC 60964: Design for control rooms of nuclear power plants. (E)
- IEC 61227: NPPs – Control rooms – Operator controls. 2008. (E)
- IEC 61771: NPPs – MCR – Design verification and validation. 1995. (E)
- IEC 61772: NPPs – MCR – Application of visual display units. 1995. (E)
- IEC 62241: NPPs – MCR – Alarm functions and presentation. 2004. (E)

Electric Power Research Institute (EPRI)

- EPRI: Human Factors Guidance for Control Room and Digital Human-System Interface. Design and Modification. 2005. (E)

Institute of Electrical and Electronic Engineers (IEEE)

- IEEE 1023: IEEE. Guide for Application of Human Factors Engineering to Systems, Equipment and Facilities of Nuclear Power Generating Systems. IEEE-1023-1988. (E)

French norms (NF)

- NF EN 897-2: Safety of machinery – Ergonomics requirements for design for means of signalling and components. (E)
- NF D 62-042: Office furniture. Tables and desk. General characteristics. Tests and requirements.
- NF D 62-041: Office furniture. Furniture storage. General characteristics. Testing and specifications.
- NF EN 527-1, NF EN 527-3: Work tables and desks.
- NF EN 1021 parts 1 and 2: Assessment of the Ignitability of Upholstered Furniture.
- NF EN 1335-1, NF EN 1335-2 and NF EN 1335-3: Office work seating.
- NF EN 13761: Visitors seating.
- NF D 65-760: Rectangular locked metal cabinets.
- AFNOR NF X35-102: Ergonomic design for the workspace in office.



UK EPR	PRE-CONSTRUCTION SAFETY REPORT	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 107 /130
		Document ID.No. UKEPR-0002-181 Issue 06

Proprietary procedures:

ENG are guidebooks for design engineer’s use. The main aim of these guidebooks is to ensure consistency and homogeneity between the various products designed.

- ENG 2-21: Degree of automation for plant systems. ECEF021855 Revision B1. EDF. May 2006. (E)
- ENG 2-31: Principles of design of synthesis information. ECEF040244 Revision D1. EDF. January 2008. (E)
- ENG 2-33: Specifications regarding the alarms. ECEF040683 Revision C1. EDF. August 2008. (E)
- ENG 2-34: Operating display format specification. ECEF040974 Revision B1. EDF. June 2006. (E)
- ENG 3-37: Design rules for operating instruction (MOP). ECEF061119 Revision A1. EDF. January 2007. (E)
- ENG 3-03 EPR Plant System Specification - Contents and Updates. ECEF050611 Revision A1. EDF. December 2005. (E)
- ENG 3-40: Content and structure of emergency operating procedures instructions. ECEF061275 Revision A1. EDF. July 2009. (E)

ECEF061275 Revision A1 is the English translation of ECEF061275 Revision A.

- Writing guide for EPR system specifications.ECEMC0000059 Revision A1. EDF. February 2010. (E)

Safety Culture:

[Ref-2] Safety Fundamentals No. SF-1: Fundamental Safety Principles. (E)

[Ref-3] Safety Requirements No. GS-R-3: The Management System for Facilities and Activities. IAEA. 2006. (E)

[Ref-4] Safety Guide No. GS-G-3.1: Application of the Management System Activities for Facilities and Activities. (E)

[Ref-5] Safety Guide No. GS-G-3.5: The Management System for Nuclear Installations. (E)

[Ref-6] Safety Series No. 75-INSAG-4: Safety Culture. (E)

[Ref-7] Safety Series No. 75-INSAG-15: Key Practical Issues in Strengthening Safety Culture. (E)

[Ref-8] Safety Report Series No. 11: Developing Safety Culture in Nuclear Activities. (E)

[Ref-9] Safety Report Series No. 42: Safety Culture in the Maintenance of Nuclear Power Plants. (E)

[Ref-10] TECDOC-1321: Self-assessment of safety culture in nuclear installations. (E)

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER : 18.1
		PAGE : 108 /130
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	Document ID.No. UKEPR-0002-181 Issue 06

[Ref-11] TECDOC-1329: Safety culture in nuclear installations. (E)

### 1.3. SCOPE

[Ref-1] UK EPR GDA Project - Reference Design Configuration. UKEPR-I-002. EDF/AREVA. (E)

[Ref-2] Human factor operating principles and benefit of computerised operation. UKEPR-0014-001 Issue 00. EDF/AREVA. December 2009. (E)

[Ref-3] State Oriented Approach designer knowledge transfer. ENFCRI090272 Revision A. EDF. November 2009. (E)

## 3. INTEGRATION OF HUMAN FACTORS INTO THE DESIGN OF THE UK EPR

[Ref-1] An overview of the Human Factors Approach used for the EPR Design and Compliance with International Standards. ECEF100427 Revision A. EDF. March 2010. (E)

### 3.1. FA3 INITIAL REFERENCE DESIGN

#### 3.1.1. General Methodology

[Ref-1] ISO. Human-centred design processes for interactive systems. ISO 13407. 1999. (E)

[Ref-2] Human Factors Engineering Programme Review Model. NUREG-0711 Revision 2. USNRC. February 2004. (E)

#### 3.1.2. Implementation of the Methodology for Allocation of Function

[Ref-1] Human factor operating principles and benefit of computerised operation. UKEPR-0014-001 Issue 00. EDF/AREVA. December 2009. (E)

[Ref-2] Summary Report on Functional Requirements Analyses per Plant System Functional requirements analysis. ECEF0100515 Revision F1. EDF. June 2010. (E)

#### 3.1.3. Implementation of the Methodology for Operation of the Plant

##### 3.1.3.2. Stage 2: Contribution to Specifications

[Ref-1] ENG 2-33 procedure: Principles for specifying and handling alarms for EPR. ECEF040683 Revision C1. EDF. August 2008. (E)

[Ref-2] EPR Operations Display Engineering Rule ENG 02-34. Operating Display format Specification. ECEF040974 Revision B1. EDF. June 2006. (E)

[Ref-3] ENG 3-37: Design rules for operating instruction (MOP). ECEF061119 Revision A1. EDF. January 2007. (E)

UK EPR	PRE-CONSTRUCTION SAFETY REPORT	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 109 /130
		Document ID.No. UKEPR-0002-181 Issue 06

[Ref-4] Procedure ENG 3-34: Content and structure of an Emergency Operating rule. ECEF061266 Revision A1. EDF. April 2009. (E)

ECEF061266 Revision A1 is the English translation of ECEF061266 Revision A.

[Ref-5] Procedure ENG 3-38: Rules for drafting normal operating rules. ECEF061353 Revision A1. EDF. May 2009. (E)

ECEF061353 Revision A1 is the English translation of ECEF061353 Revision A.

[Ref-6] ENG 2-31: Principles of design of synthesis information. ECEF040244 Revision D1. EDF. January 2008. (E)

[Ref-7] Procedure EPR ENG 3-40: Content and structure of Emergency Operating methods. ECEF061275 Revision A1. EDF. July 2009. (E)

**3.1.3.3. Stage 3: Modelling and Prototyping for review of preliminary design specifications**

[Ref-1] EPR computerised operation: Protocol for evaluation tests relative to Operation Department requirements. HT5403016 Revision A1. EDF. March 2010. (E)

HT5403016 Revision A1 is the English translation of HT5403016 Revision A.

[Ref-2] EPR HMI - Evaluation of the principles of computerised operation - Assessment of 2005 supplementary test campaign. ECEF060191 Revision A1. EDF. March 2010. (E)

ECEF060191 Revision A1 is the English translation of ECEF060191 Revision A.

[Ref-3] EPR computerised operation protocol for complementary tests. HT-54/05/021 Revision A1. EDF. March 2010. (E)

[Ref-4] Structuring of the requirements and specifications concerning the EPR Human Machine Interface. ECEF050717 Revision A1. EDF. February 2010. (E)

ECEF050717 Revision A1 is the English translation of ECEF050717 Revision A.

**3.1.3.4. Stage 4: Adjustment of Design Specifications**

[Ref-1] EPR - Technical Specifications and Conditions (CSCT) for Standard Instrumentation & Control General presentation report - CCF 01 and associated documents CCF02 to CCF17. ECECC010055 Revision F1. EDF. October 2009. (E)

ECECC010055 Revision F1 is the English translation of ECECC010055 Revision F.

[Ref-2] EPR Operations Display Engineering Rule ENG 02-34. Operating Display format Specification. ECEF040974 Revision B1. EDF. June 2006. (E)

[Ref-3] EPR Procedure ENG 3-37: Design Rules for Operating Instruction (MOP). ECEF061119 Revision A1. EDF. January 2007. (E)

[Ref-4] ENG 2-33 procedure: Principles for specifying and handling alarms for EPR. ECEF040683 Revision C1. EDF. August 2008. (E)

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 110 /130
		Document ID.No. UKEPR-0002-181 Issue 06

**[Ref-5]** Procedure EPR ENG 3-40: Content and structure of Emergency Operating methods. ECEF061275 Revision A1. EDF. July 2009. (E)

**[Ref-6]** General Policy - Guiding principles relating to the organisation of the Flamanville 3 shift crew. D4002.92-07/084. EDF. February 2010. (E)

**3.1.4. Implementation of the Methodology for Control Rooms, General Layout and Maintenance**

**3.1.4.1. Layout of Control Rooms**

**3.1.4.1.1. Stage 1: Analysis of Existing Situations**

**[Ref-1]** An overview of the Human Factors Approach used for the EPR Design and Compliance with International Standards. ECEF100427 Revision A. EDF. March 2010. (E)

**[Ref-2]** EPR room layout Analysis of activity at the Chooz (N4) nuclear power plant. 04088-300-DE-005-A1. EDF. March 2012. (E)

**3.1.4.1.2. Stage 2: Contribution to Specifications**

**[Ref-1]** Technical specifications and conditions for the layout and outfitting design of the control room, adjoining rooms, and the full scale simulator room of the EPR France plant. ECECC041294 Revision C1. EDF. February 2010. (E)

This document refers to numerous NF EN ISO or NF X standards and CEI 60964, 61771, 61839.

ECECC041294 Revision C1 is the English translation of ECECC041294 Revision C.

**[Ref-2]** EPR room layout Analysis of activity at the Chooz (N4) nuclear power plant. 04088-300-DE-005-A1. EDF. March 2012. (E)

**3.1.4.1.3. Stage 3: Modelling and Prototyping for review of preliminary design specifications**

**[Ref-1]** EPR Control Room Layout –Results of the full-scale mock-up experiment for the EPR France Control Room. 04088-300-DE006-A1. EDF. March 2012. (E)

**3.1.4.2. General Layout and Maintenance**

**3.1.4.2.1. Stage 1: Analysis of existing situations**

**3.1.4.2.1.2. Specific Human Factors Studies**

**[Ref-1]** EPR Local Maintenance and Operation Activities to be Analysed from the Human Factors Standpoint. ECEF031026 Revision B1. EDF. February 2012. (E)

**[Ref-2]** Summary and Results of the FA3 and 4 ETB Ergonomic Study. ECEP060987 Revision A1. EDF. October 2009. (E)

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>  CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	SUB-CHAPTER : 18.1
		PAGE : 111 /130
		Document ID.No. UKEPR-0002-181 Issue 06

[Ref-3] Procedure for taking into account Human Factors in Fuel Handling Operations. ECEP071048 Revision A1. EDF. February 2010. (E)

ECEP071048 Revision A1 is the English translation of ECEP071048 Revision A.

#### **3.1.4.2.2. Stage 2: Contribution to Specifications**

[Ref-1] MIP EPR No 2.64 Installation Guide - Consideration of Human Factors. ECEIG0100625 Revision B1. EDF. July 2011. (E)

[Ref-2] Fuel Building Specification. ECEIG99070 Revision B1. EDF. March 2010. (E)

## **4. SAFETY ARGUMENTS AND EVIDENCE**

### **4.1. FUNDAMENTAL DESIGN REQUIREMENTS**

#### **4.1.1. Allocation of Function**

##### **4.1.1.1. Overall Basis and Approach**

[Ref-1] Human factor operating principles and benefit of computerised operation. UKEPR-0014-001 Issue 00. EDF/AREVA. December 2009. (E)

[Ref-2] Summary Report on Functional Requirements Analyses per Plant System Functional requirements analysis. ECEF0100515 Revision F1. EDF. June 2010. (E)

##### **4.1.1.2. Automation Principles and Criteria**

[Ref-1] ENG 2-21 Procedure: Degree of automation for plant systems. ECEF021855 Revision B1. EDF. May 2006. (E)

##### **4.1.1.3. Allocation of Function for Normal Operation**

[Ref-1] ENG 2-21 Procedure: Degree of automation for plant systems. ECEF021855 Revision B1. EDF. May 2006. (E)

##### **4.1.1.5. Allocation of function for Severe Accidents**

[Ref-1] Summary Report on Functional Requirements Analyses per Plant System Functional requirements analysis. ECEF0100515 Revision F1. EDF. June 2010. (E)

##### **4.1.1.6. Human Factors Evaluation and Substantiation of Allocation of Function Choices**

[Ref-1] EPR HMI – Evaluation of the principles of computerised operation - Assessment of the 2005 supplementary test campaign. ECEF060191 Revision A1. EDF. March 2010. (E)

ECEF060191 Revision A1 is the English translation of ECEF060191 Revision A.

#### **4.1.2. Grace Periods**

[Ref-1] ENG 2-21 Procedure: Degree of automation for plant systems. ECEF021855 Revision B1. EDF. May 2006. (E)

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 112 /130
		Document ID.No. UKEPR-0002-181 Issue 06

**[Ref-2]** Safety Assessment Principles for Nuclear Facilities. UK Health and Safety Executive (HSE). 2006 Edition Revision 1. January 2008. (E)

**4.2. GENERAL DESIGN AND LAYOUT**

**4.2.1. Main Control Room**

**4.2.1.1. General Requirements and Approach**

**[Ref-1]** Technical specifications and conditions for the layout and outfitting design of the control room, adjoining rooms, and the full scale simulator room of the EPR France plant. ECECC041294 Revision C1. EDF. February 2010. (E)

This document refers to numerous NF EN ISO or NF X standards and CEI 60964, 61771, 61839.

ECECC041294 Revision C1 is the English translation of ECECC041294 Revision C.

**[Ref-2]** EPR room layout Analysis of activity at the Chooz (N4) nuclear power plant. 04088-300-DE-005-A1. EDF. March 2012. (E)

**[Ref-3]** International Standards, Guidelines and Technical Guidelines:

International Organisation for Standardisation (ISO)

- ISO 9241-210: Ergonomics of Human-System Interaction - Part 210: Human-Centred Design for interactive Systems. 2010. (E)
- ISO 11064: Ergonomic design of control centres. 2008. (E)
- ISO 9241: Ergonomics of human system interaction. 2002. (E)
- ISO 80416: Basic principles for graphical symbols for use on equipment. 2005. (E)
- ISO 7000: Graphical for use on equipment. 2004. (E)
- ISO 14617: Graphical symbols for diagrams. 2004. (E)
- ISO 13406: Ergonomic requirements for work on flat panel display screens. (E)
- ISO 15534: Ergonomic design for the safety of machinery. 2000. (E)
- ISO 14738: Safety of machinery – anthropometric requirements for the design of workstations at machinery. 2002. (E)
- ISO 6385: Ergonomics principles in the design of work systems. 1990. (E)

Nuclear Regulatory Commission (NRC)

- NUREG-0700: Human-System Interface Design Review Guidelines. Revision 2. 2002. (E)
- NUREG-0711: Human Factors Engineering Program Review Model. Revision 2. February 2004. (E)

UK EPR	PRE-CONSTRUCTION SAFETY REPORT	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 113 /130
		Document ID.No. UKEPR-0002-181 Issue 06

- NUREG-0800 Chapter 18. Human Factors Engineering. Revision 2. 2004. (E)
- NUREG/CR-6633: Advanced Information Systems: Technical Basis and Human Factors Review Guidance. 2000. (E)
- NUREG/CR-6634: Computer-Based Procedure Systems: Technical Basis and Human Factors Review Guidance. 2000. (E)
- NUREG/CR-6635: Soft Controls: Technical Basis and Human Factors Review Guidance. 2000. (E)
- NRC NUREG-1764: Guidance for the Review of Changes to Human Actions. 2004. (E)

International Electrotechnical Commission (IEC)

- IEC 80416: Basic principles for graphical symbols for use on equipment. 2002. (E)
- IEC 61839: Nuclear Power Plants - Design of control rooms - Functional analysis and assignment. November 2000. (E)
- IEC 60073: Basic and safety principles for man-machine interfaces, marking and identification. 2002. (E)
- IEC 60447: Man-machine interface – actuating principles. 2004. (E)
- IEC 60960: Functional design criteria for SPDS. 1988. (E)
- IEC 60964: Design for control rooms of nuclear power plants. (E)
- IEC 61227: NPPs – Control rooms – Operator controls. 2008. (E)
- IEC 61771: NPPs – MCR – Design verification and validation. 1995. (E)
- IEC 61772: NPPs – MCR – Application of visual display units. 1995. (E)
- IEC 62241: NPPs – MCR – Alarm functions and presentation. 2004. (E)

Electric Power Research Institute (EPRI)

- EPRI: Human Factors Guidance for Control Room and Digital Human-System Interface. Design and Modification. 2005. (E)

Institute of Electrical and Electronic Engineers (IEEE)

- IEEE 1023: IEEE. Guide for Application of Human Factors Engineering to Systems, Equipment and Facilities of Nuclear Power Generating Systems. IEEE-1023-1988. (E)

French norms (NF)

- NF EN 897-2: Safety of machinery – Ergonomics requirements for design for means of signalling and components. (E)
- NF D 62-042: Office furniture. Tables and desk. General characteristics. Tests and requirements.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 114 /130
		Document ID.No. UKEPR-0002-181 Issue 06

- NF D 62-041: Office furniture. Furniture storage. General characteristics. Testing and specifications.
- NF EN 527-1, NF EN 527-3: Work tables and desks.
- NF EN 1021 parts 1 and 2: Assessment of the Ignitability of Upholstered Furniture.
- NF EN 1335-1, NF EN 1335-2 and NF EN 1335-3: Office work seating.
- NF EN 13761: Visitors seating.
- NF D 65-760: Rectangular locked metal cabinets.
- AFNOR NF X35-102: Ergonomic design for the workspace in office.

Proprietary procedures:

ENG are guidebooks for design engineer's use. The main aim of these guidebooks is to ensure consistency and homogeneity between the various products designed.

- ENG 2-21: Degree of automation for plant systems. ECEF021855 Revision B1. EDF. May 2006. (E)
- ENG 2-31: Principles of design of synthesis information. ECEF040244 Revision D1. EDF. January 2008. (E)
- ENG 2-33: Specifications regarding the alarms. ECEF040683 Revision C1. EDF. August 2008. (E)
- ENG 2-34: Operating display format specification. ECEF040974 Revision B1. EDF. June 2006. (E)
- ENG 3-37: Design rules for operating instruction (MOP). ECEF061119 Revision A1. EDF. January 2007. (E)
- ENG 3-03 EPR Plant System Specification - Contents and Updates. ECEF050611 Revision A1. EDF. December 2005. (E)
- ENG 3-40: Content and structure of emergency operating procedures instructions. ECEF061275 Revision A1. EDF. July 2009. (E)

ECEF061275 Revision A1 is the English translation of ECEF061275 Revision A.

- Writing guide for EPR system specifications.ECEMC0000059 Revision A1. EDF. February 2010. (E)

**[Ref-4]** EPR Control Room Layout –Results of the full-scale mock-up experiment for the EPR France Control Room. 04088-300-DE006-A1. EDF. March 2012. (E)

**4.2.1.2. General Design and Layout of the MCR**

**[Ref-1]** Class 1 Control and Display Facilities in the Main Control Room and the Remote Shutdown Station. ECECC111829 Revision B. EDF. August 2012. (E)



<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 115 /130
		Document ID.No. UKEPR-0002-181 Issue 06

**4.2.1.3. Specific Design Considerations for the MCR**

**4.2.1.3.1. Situational Awareness**

**[Ref-1]** Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors. 37(1). 32-54. Endsley. 1995b.

**[Ref-2]** EPR room layout. Analysis of activity at the Chooz (N4) nuclear power plant. 04088-300-DE-005-A1. EDF. March 2012. (E)

**4.2.1.3.2. Communication and Collaborative Working**

**[Ref-1]** EPR room layout Analysis of activity at the Chooz (N4) nuclear power plant. 04088-300-DE-005-A1. EDF. March 2012. (E)

**[Ref-2]** Technical specifications and conditions for the layout and outfitting design of the control room, adjoining rooms, and the full scale simulator room of the EPR France plant. ECECC041294 Revision C1. EDF. February 2010. (E)

This document refers to numerous NF EN ISO or NF X standards and CEI 60964, 61771, 61839.

ECECC041294 Revision C1 is the English translation of ECECC041294 Revision C.

**4.2.1.3.3. MCR Working Environment**

**[Ref-1]** Technical specifications and conditions for the layout and outfitting design of the control room, adjoining rooms, and the full scale simulator room of the EPR France plant. ECECC041294 Revision C1. EDF. February 2010. (E)

This document refers to numerous NF EN ISO or NF X standards and CEI 60964, 61771, 61839.

ECECC041294 Revision C1 is the English translation of ECECC041294 Revision C.

**[Ref-2]** Sheet C5 "Control Rooms and Annexes". ECEIG0100002 Revision A1. EDF. March 2010. (E)

**[Ref-3]** EPR room layout Analysis of activity at the Chooz (N4) nuclear power plant. 04088-300-DE-005-A1. EDF. March 2012. (E)

**4.2.2. Remote Shutdown Station**

**[Ref-1]** Technical specifications and conditions for the layout and outfitting design of the control room, adjoining rooms, and the full scale simulator room of the EPR France plant. ECECC041294 Revision C1. EDF. February 2010. (E)

This document refers to numerous NF EN ISO or NF X standards and CEI 60964, 61771, 61839.

ECECC041294 Revision C1 is the English translation of ECECC041294 Revision C.

**[Ref-2]** Habitability of the main control room in the event of fire. ECEF051003 Revision A1. EDF. October 2008. (E)

UK EPR	PRE-CONSTRUCTION SAFETY REPORT	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 116 /130
		Document ID.No. UKEPR-0002-181 Issue 06

[Ref-3] EPR room layout Analysis of activity at the Chooz (N4) nuclear power plant. 04088-300-DE-005-A1. EDF. March 2012. (E)

**4.2.3. Emergency Management Facilities**

[Ref-1] Technical specifications and conditions for the layout and outfitting design of the control room, adjoining rooms, and the full scale simulator room of the EPR France plant. ECECC041294 Revision C1. EDF. February 2010. (E)

This document refers to numerous NF EN ISO or NF X standards and CEI 60964, 61771, 61839.

ECECC041294 Revision C1 is the English translation of ECECC041294 Revision C.

[Ref-2] EPR room layout Analysis of activity at the Chooz (N4) nuclear power plant. 04088-300-DE-005-A1. EDF. March 2012. (E)

**4.2.4. Other UK EPR Buildings and Facilities**

[Ref-1] EPR Local Maintenance and Operation Activities to be Analysed from the Human Factors Standpoint. ECEF031026 Revision B1. EDF. February 2012. (E)

**4.2.4.1. Working Environment**

[Ref-1] Technical specifications and conditions for the layout and outfitting design of the control room, adjoining rooms, and the full scale simulator room of the EPR France plant. ECECC041294 Revision C1. EDF. February 2010. (E)

This document refers to numerous NF EN ISO or NF X standards and CEI 60964, 61771, 61839.

ECECC041294 Revision C1 is the English translation of ECECC041294 Revision C.

[Ref-2] EPR room layout Analysis of activity at the Chooz (N4) nuclear power plant. 04088-300-DE-005-A1. EDF. March 2012. (E)

[Ref-3] Specifications for Nuclear Auxiliary Building. ECEIG0000333 Revision E1. EDF. February 2008. (E)

[Ref-4] Specifications for Safeguard Auxiliary and Electrical Buildings. ECEIG0000810 Revision C1. EDF. January 2010. (E)

[Ref-5] A Meziere, P Bily. Reactor Building Specification. ECEIG0001089 Revision C1. EDF. September 2009. (E)

ECEIG0001089 Revision C1 is the English translation of ECEIG0001089 Revision C.

[Ref-6] Diesel Building: Specifications of the Diesels Buildings ECEIG0000756 Revision C1. EDF. February 2009. (E)

[Ref-7] Fuel Building Specification. ECEIG99070 Revision B1. EDF. March 2010. (E)

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER : 18.1
		PAGE : 117 /130
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	Document ID.No. UKEPR-0002-181 Issue 06

#### 4.2.4.3. Local-to-Plant Activities and Layout

- [Ref-1]** Note EPR Optimisation des chantiers Radioprotection hors BR  
[EPR Optimisation of activities with Radiation Protection Level other than the BR].  
ECEIG021333 Revision A. EDF. November 2003. (F/E)
- This document is available in French and is included for information only.
- [Ref-2]** EPR Optimisation of activities with Radiation Protection Level – Thermal insulation removal and reinstallation – phase 2.  
EYRL/2008/fr/0003 Revision D1. EDF. June 2010. (E)
- [Ref-3]** EPR Optimisation of activities with Radiation Protection Level – Site Logistics – phase 2. EYRL/2008/fr/0048 Revision C1. EDF. February 2010. (E)
- [Ref-4]** EPR - optimisation of activities that impact radiation protection - RCP, RCV and RIS/RRA valves - volume 2. ECEMA071469 Revision C1. EDF. May 2010. (E)
- [Ref-5]** EPR - Optimizing radiation protection-related activities - preparing and inspecting steam generators - Chapter 2. ECEMA070805 Revision B1. EDF. April 2010. (E)
- [Ref-6]** EPR - Optimizing radioprotection-related activities - opening/closing reactor vessel head activity - Chapter 2. ECEMA070986 Revision B1. EDF. April 2010. (E)
- [Ref-7]** EPR Optimisation of activities with Radiation Protection impact fuel shipment – chapter 2 – YR2621. EYTM/2007/fr/0030 Revision C1. EDF. June 2010. (E)
- [Ref-8]** EPR Optimisation of Radioprotection activities. Waste treatment Phase 1 and 2. D4002.92-06/123 Revision 0.1. EDF. March 2009. (E)
- [Ref-9]** Review of the FA3 PDMS model of the installation levels +13.40m and +15.20m of the nuclear Auxiliary Building. ECEIG100655 Revision A. EDF. June 2010. (E)
- [Ref-10]** Review of the FA3 PDMS model of the installation level +3.70m of the Nuclear Auxiliary Building. ECEIG091382 Revision A. EDF. July 2009. (E)
- [Ref-11]** EPR Optimisation of activities with Radiation Protection Level – Thermal insulation removal and reinstallation. ECEIG040462 Revision B1. EDF. January 2006. (E)
- [Ref-12]** EPR Optimisation of activities with Radiation Protection Level – Site Logistics. ECEIG041062 Revision B1. EDF. January 2009. (E)
- [Ref-13]** EPR Optimisation of activities with Radiation Protection risk – RCP, RCV, RIS/RRA. ECEMA050230 Revision B1. EDF. January 2009. (E)
- [Ref-14]** EPR Optimisation of activities with Radiation Protection Level – Preparation and control Steam Generators – Phase 1. ECEMA041034 Revision B1. EDF. March 2009. (E)
- [Ref-15]** EPR Optimisation of activities with Radiation Protection Level – Opening /Closure reactor vessel – Phase 1. ECEMA050275 Revision C1. EDF. February 2009. (E)
- [Ref-16]** EPR Optimisation of activities with Radiation Protection Level – Fuel posting out activities – Phase 1. ECEMA050056 Revision A1. EDF. March 2009. (E)

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 118 /130
		Document ID.No. UKEPR-0002-181 Issue 06

**[Ref-17]** EPR Optimisation of Radioprotection activities. Waste treatment Phases 1 and 2. D4002.92-06/123 Revision 0.1. EDF. March 2009. (E)

**[Ref-18]** Specifications for Safeguard Auxiliary and Electrical Buildings. ECEIG0000810 Revision C1. EDF. January 2010. (E)

**[Ref-19]** A Meziere, P Bily. Reactor Building Specification. ECEIG0001089 Revision C1. EDF. September 2009. (E)

ECEIG0001089 Revision C1 is the English translation of ECEIG0001089 Revision C.

**[Ref-20]** Diesel Building: Specifications of the Diesels Buildings. ECEIG0000756 Revision C1. EDF. February 2009. (E)

**[Ref-21]** Fuel Building Specification. ECEIG99070 Revision B1. EDF. March 2010. (E)

**4.2.4.5. Integration of the results into the Design**

**[Ref-1]** Specifications for Nuclear Auxiliary Building. ECEIG0000333 Revision E1. EDF. February 2008. (E)

**[Ref-2]** Specifications for Safeguard Auxiliary and Electrical Buildings. ECEIG0000810 Revision C1. EDF. January 2010. (E)

**[Ref-3]** A Meziere, P Bily. Reactor Building Specification. ECEIG0001089 Revision C1. EDF. September 2009. (E)

ECEIG0001089 Revision C1 is the English translation of ECEIG0001089 Revision C.

**[Ref-4]** Diesel Building: Specifications of the Diesels Buildings. ECEIG0000756 Revision C1. EDF. February 2009. (E)

**[Ref-5]** Fuel Building Specification. ECEIG99070 Revision B1. EDF. March 2010. (E)

**[Ref-6]** EPR ENG 3-06 - Guide de rédaction des cahiers des charges (CdC) des bâtiments [Procedure ENG 3-06 – Building Specification Writing Guide]).

This document is only available in French and is provided for information only.

**[Ref-7]** MIP EPR No 2.64 Installation Guide - Consideration of Human Factors. ECEIG0100625 Revision B1. EDF. July 2011. (E)

**4.3. HUMAN-MACHINE INTERFACE DESIGN**

**[Ref-1]** UK EPR GDA Project - Reference Design Configuration. UKEPR-I-002. EDF/AREVA. (E)

**4.3.1. Overall Basis, Principles and Requirements**

**[Ref-1]** NS-R-1 - Safety of Nuclear Power Plants: Design (Requirements). 2000. (E)

**[Ref-2]** NS-G-1.1 - Software for Computer Based Systems Important for Safety in Nuclear Power Plants. 2000. (E)

UK EPR	PRE-CONSTRUCTION SAFETY REPORT	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 119 /130
		Document ID.No. UKEPR-0002-181 Issue 06

[Ref-3] NS-G-1.3 - Instrumentation and Control Systems Important to Safety in Nuclear Power Plants. 2002. (E)

[Ref-4] International Standard Guidelines and Technical Guidelines:

International Organisation for Standardisation (ISO)

- ISO 9241-210: Ergonomics of Human-System Interaction - Part 210: Human-Centred Design for interactive Systems. 2010. (E)
- ISO 11064: Ergonomic design of control centres. 2008. (E)
- ISO 9241: Ergonomics of human system interaction. 2002. (E)
- ISO 80416: Basic principles for graphical symbols for use on equipment. 2005. (E)
- ISO 7000: Graphical for use on equipment. 2004. (E)
- ISO 14617: Graphical symbols for diagrams. 2004. (E)
- ISO 13406: Ergonomic requirements for work on flat panel display screens. (E)
- ISO 15534: Ergonomic design for the safety of machinery. 2000. (E)
- ISO 14738: Safety of machinery – anthropometric requirements for the design of workstations at machinery. 2002. (E)
- ISO 6385: Ergonomics principles in the design of work systems. 1990. (E)

**4.3.2. HMI in the Main Control Room**

**4.3.2.1. Main Operating HMIs**

**4.3.2.1.1. MCP [PICS] Workstations**

[Ref-1] EPR - Technical Specifications and Conditions (CSCT) for Standard Instrumentation & Control General presentation report - CCF 01 and associated documents CCF02 to CCF17. ECECC010055 Revision F1. EDF. October 2009. (E)

ECECC010055 Revision F1 is the English translation of ECECC010055 Revision F.

4.3.2.1.1.1. Human Factors input to the design and evaluation of the MCP [PICS]

[Ref-1] Task model analysis for operating activities. D455010054528 Revision 0. EDF. December 2005. (E)

[Ref-2] Structuring of the requirements and specifications concerning the EPR Human-Machine Interface (HMI). ECEF050717 Revision A1. EDF. February 2010. (E)

ECEF050717 Revision A1 is the English translation of ECEF050717 Revision A.

[Ref-3] ENG 3-03 EPR Plant System Specification - Contents and Updates. ECEF050611 Revision A1. EDF. December 2005. (E)

UK EPR	PRE-CONSTRUCTION SAFETY REPORT	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 120 /130
		Document ID.No. UKEPR-0002-181 Issue 06

[Ref-4] EPR computerised operation protocol for complementary tests. HT-54/05/021 Revision A1. EDF. March 2010. (E)

[Ref-5] EPR Operations Display Engineering Rule ENG 02-34. Operating Display format Specification. ECEF040974 Revision B1. EDF. June 2006. (E)

4.3.2.1.1.2. Organisation and composition of the MCP [PICS] displays

[Ref-1] Task model analysis for operating activities. D455010054528 Revision 0. EDF. December 2005. (E)

[Ref-2] Structuring of the requirements and specifications concerning the EPR Human-Machine Interface (HMI). ECEF050717 Revision A1. EDF. February 2010. (E)

ECEF050717 Revision A1 is the English translation of ECEF050717 Revision A.

[Ref-3] EPR Operations Display Engineering Rule ENG 02-34. Operating Display format Specification. ECEF040974 Revision B1. EDF. June 2006. (E)

[Ref-4] Human factor operating principles and benefit of computerised operation. UKEPR-0014-001 Issue 00. EDF/AREVA. December 2009. (E)

4.3.2.1.1.4. Input Devices and Navigation

[Ref-1] Human factor operating principles and benefit of computerised operation. UKEPR-0014-001 Issue 00. EDF/AREVA. December 2009. (E)

4.3.2.1.2. Protection System Operator Terminal

[Ref-1] Protection System Operator Terminal Basis of Safety Case. ECECC120489 Revision A. EDF. May 2012. (E)

4.3.2.1.4. Plant Overview Panel (POP)

[Ref-1] Human factor operating principles and benefit of computerised operation. UKEPR-0014-001 Issue 00. EDF/AREVA. December 2009. (E)

[Ref-2] EPR Operations Display Engineering Rule ENG 02-34. Operating Display format Specification. ECEF040974 Revision B1. EDF. June 2006. (E)

[Ref-3] Feasibility study of Operation Division specifications for EPR computerised operation. ECEF032026 Revision A1. EDF. September 2010. (E)

[Ref-4] Structuring of the requirements and specifications concerning the EPR Human-Machine Interface (HMI). ECEF050717 Revision A1. EDF. February 2010. (E)

ECEF050717 Revision A1 is the English translation of ECEF050717 Revision A.

4.3.2.1.5. Inter-Panel Signalisation Panel (PSIS)

[Ref-1] Class 1 Control and Display Facilities in the Main Control Room and the Remote Shutdown Station. ECECC111829 Revision B. EDF. August 2012. (E)

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 121 /130
		Document ID.No. UKEPR-0002-181 Issue 06

**4.3.2.2. Back-up Control System HMIs**

**4.3.2.2.1. MCS [SICS] Panel**

**[Ref-1]** Class 1 Control and Display Facilities in the Main Control Room and the Remote Shutdown Station. ECECC111829 Revision B. EDF. August 2012. (E)

**[Ref-2]** PICS to SICS Transfer: A claims, arguments and evidence-based safety case. 16895-707-000-RPT-0017 Revision G-BPE. AMEC. August 2012. (E)

**[Ref-3]** Sizing of SICS. ECEF021069 Revision E1. EDF. December 2010. (E)

**[Ref-4]** SICS Operating Principles. ENFCRI090069 Revision A. EDF. March 2009. (E)

ENFCRI090069 Revision A is the English translation of ENFCRI070019 Revision B.

**[Ref-5]** Human factor operating principles and benefit of computerised operation. UKEPR-0014-001 Issue 00. EDF/AREVA. December 2009. (E)

**[Ref-6]** Task model analysis for operating activities. D455010054528 Revision 0. EDF. December 2005. (E)

**[Ref-7]** Structuring of the requirements and specifications concerning the EPR Human-Machine Interface (HMI). ECEF050717 Revision A1. EDF. February 2010. (E)

ECEF050717 Revision A1 is the English translation of ECEF050717 Revision A.

**[Ref-8]** EDF/AREVA GDA Task Analysis: Entry into Severe Accident Management Guidelines (OSSA). 16895-707-000-RPT-0006 Revision E-BPE. AMEC. August 2012. (E)

**4.3.2.2.2. Non-Computerised Safety System (NCSS)**

**[Ref-1]** Non-Computerised Safety System - Basis of Safety Case. PTL-F DC 5 Revision A. AREVA. August 2012. (E)

**[Ref-2]** EPR UK Functional Requirements on Non-Computerised Safety I&C Functions. NEPR-F DC 551 Revision C. AREVA. July 2012. (E)

**[Ref-3]** Safety Requirements for Non-Computerised Safety System (NCSS). NEPS-F DC 555 Revision D. AREVA. June 2012. (E)

**[Ref-4]** EDF/AREVA GDA Task Analysis: Operator responses to decreasing RCS level (OP\_SIS\_INJ\_80MN\_NCSS) on the Non Computerised Safety System. 16895-707-000-RPT-0010 Revision G-BPE. AMEC. October 2012. (E)

**4.3.3. Alarms**

**4.3.3.1. Principles and Requirements**

**[Ref-1]** ENG 2-33: Specifications regarding the alarms. ECEF040683 Revision C1. EDF. August 2008. (E)

**[Ref-2]** Human factor operating principles and benefit of computerised operation. UKEPR-0014-001 Issue 00. EDF/AREVA. December 2009. (E)

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 122 /130
		Document ID.No. UKEPR-0002-181 Issue 06

**[Ref-3]** EPR computerised operation protocol for complementary tests. HT-54/05/021 Revision A1. EDF. March 2010. (E)

**[Ref-4]** EPR HMI – Evaluation of the principles of computerised operation - Assessment of the 2005 supplementary test campaign. ECEF060191 Revision A1. EDF. March 2010. (E)

ECEF060191 Revision A1 is the English translation of ECEF060191 Revision A.

**[Ref-5]** ENG 3-03 EPR Plant System Specification - Contents and Updates. ECEF050611 Revision A1. EDF. December 2005. (E)

**4.3.3.2. Alarm Classification**

**[Ref-1]** ENG 2-33: Specifications regarding the alarms. ECEF040683 Revision C1. EDF. August 2008. (E)

**4.3.3.3. Automatic Diagnosis Annunciation**

**[Ref-1]** EPR HMI – Evaluation of the principles of computerised operation - Assessment of the 2005 supplementary test campaign. ECEF060191 Revision A1. EDF. March 2010. (E)

ECEF060191 Revision A1 is the English translation of ECEF060191 Revision A.

**4.3.3.5. MCP [PICS] Alarms**

**[Ref-1]** ENG 2-33: Specifications regarding the alarms. ECEF040683 Revision C1. EDF. August 2008. (E)

**4.3.3.6. MCS [SICS] Alarms**

**[Ref-1]** ENG 2-33 procedure: Principles for specifying and handling alarms for EPR. ECEF040683 Revision C1. EDF. August 2008. (E)

**[Ref-2]** Sizing of SICS. ECEF021069 Revision E1. EDF. December 2010. (E)

**4.3.4. Non-MCR and Local Controls and Indications**

**4.3.4.1. HMI in the RSS and TSC**

**4.3.4.1.1. RSS**

**[Ref-1]** Class 1 Control and Display Facilities in the Main Control Room and the Remote Shutdown Station. ECECC111829 Revision B. EDF. August 2012. (E)

**4.4. OPERATING TEAM STAFFING CONCEPT**

**4.4.1. Guiding Principles**

**[Ref-1]** General Policy - Guiding principles relating to the organisation of the Flamanville 3 shift crew. D4002.92-07/084. EDF. February 2010. (E)



<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 123 /130
		Document ID.No. UKEPR-0002-181 Issue 06

#### 4.4.2. Operating Team Composition and Minimum Shift Complement

##### 4.4.2.1. Operating Team Composition

**[Ref-1]** General Policy - Guiding principles relating to the organisation of the Flamanville 3 shift crew. D4002.92-07/084. EDF. February 2010. (E)

**[Ref-2]** EPR HMI – Evaluation of the principles of computerised operation - Assessment of the 2005 supplementary test campaign. ECEF060191 Revision A1. EDF. March 2010. (E)

ECEF060191 Revision A1 is the English translation of ECEF060191 Revision A.

##### 4.4.2.2. Minimum Shift Complement

**[Ref-1]** General Policy - Guiding principles relating to the organisation of the Flamanville 3 shift crew. D4002.92-07/084. EDF. February 2010. (E)

#### 4.4.3. Roles and Responsibilities

**[Ref-1]** General Policy - Guiding principles relating to the organisation of the Flamanville 3 shift crew. D4002.92-07/084. EDF. February 2010. (E)

**[Ref-2]** EPR computerised operation protocol for complementary tests. HT-54/05/021 Revision A1. EDF. March 2010. (E)

**[Ref-3]** EPR HMI – Evaluation of the principles of computerised operation - Assessment of the 2005 supplementary test campaign. ECEF060191 Revision A1. EDF. March 2010. (E)

ECEF060191 Revision A1 is the English translation of ECEF060191 Revision A.

##### 4.4.3.3. Safety Engineer

##### 4.4.3.3.2. Emergency Operation

**[Ref-1]** General Policy - Guiding principles relating to the organisation of the Flamanville 3 shift crew. D4002.92-07/084. EDF. February 2010. (E)

#### 4.4.4. Human Factors Validation of the Operating Team Staffing Concept

##### 4.4.4.1. FA3 HFE Programme

**[Ref-1]** EPR HMI – Evaluation of the principles of computerised operation - Assessment of the 2005 supplementary test campaign. ECEF060191 Revision A1. EDF. March 2010. (E)

ECEF060191 Revision A1 is the English translation of ECEF060191 Revision A.

### 4.5. UK EPR PROCEDURE CONCEPT

#### 4.5.1. Summary of the UK EPR Procedure Concept

**[Ref-1]** Procedure ENG 3-38: Rules for drafting normal operating rules ECEF061353 Revision A1. EDF. May 2009. (E)

ECEF061353 Revision A1 is the English translation of ECEF061353 Revision A.

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 124 /130
		Document ID.No. UKEPR-0002-181 Issue 06

**[Ref-2]** Human factor operating principles and benefit of computerised operation. UKEPR-0014-001 Issue 00. EDF/AREVA. December 2009. (E)

**4.5.2. Normal Operating Procedures**

**[Ref-1]** Human factor operating principles and benefit of computerised operation. UKEPR-0014-001 Issue 00. EDF/AREVA. December 2009. (E)

**[Ref-2]** Procedure ENG 3-38: Rules for drafting normal operating rules. ECEF061353 Revision A1. EDF. May 2009. (E)

**[Ref-3]** EPR Procedure ENG 3-37: Design Rules for Operating Instruction (MOP). ECEF061119 Revision A1. EDF. January 2007. (E)

**4.5.3. Emergency Procedures**

**4.5.3.2. Development, Verification and Validation of Emergency Operating Principles and Procedures**

**4.5.3.2.1. FA3 Initial Reference Design**

**[Ref-1]** EPR HMI – Evaluation of the principles of computerised operation - Assessment of the 2005 supplementary test campaign. ECEF060191 Revision A1. EDF. March 2010. (E)

ECEF060191 Revision A1 is the English translation of ECEF060191 Revision A.

**[Ref-2]** EPR Emergency Operation Process – Interface with qualification. ECEF070498 Revision A1. EDF. July 2009. (E)

ECEF070498 Revision A1 is the English translation of ECEF070498 Revision A.

**[Ref-3]** Procedure ENG 3-34: Content and structure of an Emergency Operating rule. ECEF061266 Revision A1. EDF. April 2009. (E)

ECEF061266 Revision A1 is the English translation of ECEF061266 Revision A.

**[Ref-4]** ENG 3-40: Content and structure of emergency operating procedures instructions. ECEF061275 Revision A1. EDF. July 2009. (E)

ECEF061275 Revision A1 is the English translation of ECEF061275 Revision A.

**4.5.5. Misdiagnosis Potential**

**[Ref-1]** Holistic Arguments and Evidence to Support Claims relating to Misdiagnosis in Emergency Operations. 16895-707-000-RPT-0015 Revision F-BPE. AMEC. August 2012. (E)

**4.5.6. Violation Potential**

**[Ref-1]** UK EPR Human Factors: Potential for mis-diagnosis and potential for violation. ECEF110313 Revision A. EDF. March 2011. (E)

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER : 18.1
		PAGE : 125 /130
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	Document ID.No. UKEPR-0002-181 Issue 06

## **5. IDENTIFICATION AND SUBSTANTIATION OF HUMAN BASED SAFETY CLAIMS**

### **5.1. OVERALL RISK SIGNIFICANCE OF HUMAN BASED SAFETY CLAIMS**

**[Ref-1]** UK EPR – Identification and categorisation of PSA 2011 type C claims. PEPSPF/11.304. F Godefroy. AREVA. July 2011. (E)

### **5.2. OVERVIEW AND BASIS FOR APPROACH**

**[Ref-1]** Confirmation of Design Features Relating to Misalignment of Automated Valves. PEPSPF/11.486 Revision 1. AREVA. December 2011. (E)

**[Ref-2]** Technical Assessment Guide - Human Reliability Analysis. T/AST/063 Issue 1. UK Health and Safety Executive (HSE). 2009. (E)

**[Ref-3]** NUREG 1764. Guidance for the Review of Changes to Human Actions. 2004. (E)

**[Ref-4]** Safety Assessment Principles for Nuclear Facilities. UK Health and Safety Executive (HSE). 2006 Edition Revision 1. January 2008. (E)

**[Ref-5]** EDF/AREVA GDA Task Analysis : Method statement and analysis of two example operators claims. 16474/TR/0003 Issue D-BPE. AMEC. May 2012. (E)

### **5.3. HUMAN BASED SAFETY CLAIMS IN THE PSA**

#### **5.3.1. Summary of Overall HRA Methodology**

**[Ref-1]** Safety Assessment Principles for Nuclear Facilities. UK Health and Safety Executive (HSE). 2006 Edition Revision 1. January 2008. (E)

**[Ref-2]** Technical Assessment Guide - Human Reliability Analysis. T/AST/063 Issue 1. UK Health and Safety Executive (HSE). 2009. (E)

**[Ref-3]** Confirmation of Design Features Relating to Misalignment of Automated Valves. PEPSPF/11.486 Revision 1. AREVA. December 2011. (E)

**[Ref-4]** Human Reliability Analysis Notebook of the UK EPR Probabilistic Safety Assessment. NEPS-F DC 191 Revision A. AREVA. January 2010. (E)

**[Ref-5]** E Sauvage. UK EPR Level 2 Supporting Human Reliability Analysis. NEPS-F DC 527 Revision A FIN. AREVA. January 2010. (E)

**[Ref-6]** A D Swain. Accident Sequence Evaluation Program Human Reliability Analysis Procedure. NUREG/CR-4772. Sandia National Laboratories. Albuquerque. New Mexico. February 1987. (E)

**[Ref-7]** A D Swain and H E Guttman. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications – Final Report. NUREG/CR-1278. Sandia National Laboratories. August 1983. (E)

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 126 /130
		Document ID.No. UKEPR-0002-181 Issue 06

**[Ref-8]** The SPAR-H Human Reliability Analysis Method. NUREG/CR-6883. Idaho National Laboratory. August 2005. (E)

**[Ref-9]** NUREG 1792. Good Practices for Implementing Human Reliability Analysis. 2005. (E)

**5.3.2. Identification and substantiation of Pre-fault HBSCs for systems and equipment modelled in the PSA (Type A and B)**

**5.3.2.1. Type A**

**[Ref-1]** Task Analysis Methodology: Analysis of Type A and B Pre-fault Human Errors. 17163-707-000-RPT-0001 Issue 06. AMEC. September 2011. (E)

**[Ref-2]** List of Significant Equipment and Failure Modes for Pre-accident HFE analysis. PEPSPF/11.336. AREVA. August 2011. (E)

**[Ref-3]** A Wilkinson. UK GDA Analysis of Pre-Initiator Human Errors. Risk Significant Equipment Types Grouped by Generic Equipment Type (Including Legacy – Non-Legacy Status). 17163-190-000-RPT-0001 Issue 02. AMEC. August 2011. (E)

**[Ref-4]** Identification of Tasks Associated with Type A/B Human Failure Events Modelled in the PSA. 17163-707-000-RPT-0002 Issue F-BPE. AMEC. February 2012. (E)

**[Ref-5]** Substantiation of Identified Type A Human Failure Events Modelled in the PSA. 17163-707-000-RPT-0004 Revision H-BPE. AMEC. August 2012. (E)

**5.3.2.2. Type B**

**[Ref-1]** EPR UK GDA Issue HF01- report D1.7: Substantiation of Identified Type B Human Failure Events. ECESN120755 Revision A. EDF. November 2012. (E)

**5.3.3. Identification and Substantiation of Post-fault HBSCs (Type C)**

**5.3.3.1. Identification and substantiation of post-fault HBSCs (Type C) in the PSA**

**[Ref-1]** EDF/AREVA GDA Task Analysis : Method statement and analysis of two example operators claims. 16474/TR/0003 Issue D-BPE. AMEC. May 2012. (E)

**5.3.3.2. Categorisation of Type C HBSCs**

**[Ref-1]** Human Reliability Analysis Notebook of the UK EPR Probabilistic Safety Assessment. NEPS-F DC 191 Revision A. AREVA. January 2010. (E)

**[Ref-2]** E.Sauvage. UK EPR Level 2 Supporting Human Reliability Analysis. NEPS-F DC 527 Revision A FIN. AREVA. January 2010. (E)

**[Ref-3]** EDF/AREVA GDA Task Analysis : Method statement and analysis of two example operators claims. 16474/TR/0003 Issue D-BPE. AMEC. May 2012. (E)

**[Ref-4]** NRC NUREG-1764: Guidance for the Review of Changes to Human Actions. 2004. (E)

**[Ref-5]** UK EPR – Identification and categorisation of PSA 2011 type C claims. PEPSPF/11.304. AREVA. July 2011. (E)

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 127 /130
		Document ID.No. UKEPR-0002-181 Issue 06

**[Ref-6]** Confirmation of design features related to claims M3/M23/M25/M28. PEPSF/12.104 Revision 1. AREVA. March 2012. (E)

**5.3.3.3. Substantiation**

**[Ref-1]** EDF/AREVA GDA Task Analysis : Method statement and analysis of two example operators claims. 16474/TR/0003 Issue D-BPE. AMEC. May 2012. (E)

**[Ref-2]** L Ainsworth et al. Guidelines for the Selection and Use of Task Analysis Data in the UK Nuclear Industry. HF/GNSR/5028 Revision B. February 2000. (E)

**5.3.3.4. Summary of Results**

**[Ref-1]** EDF/AREVA GDA Task Analysis : Method statement and analysis of two example operators claims. 16474/TR/0003 Issue D-BPE. AMEC. May 2012. (E)

**[Ref-2]** EDF/AREVA GDA Task Analysis: Post Fault Example 3 [OP\_FEED\_TK]. 16474/TR/0006 Issue G-BPE. AMEC. May 2012. (E)

**[Ref-3]** EDF/AREVA GDA Task Analysis: Feed and Bleed Recovery Strategies [OP\_BLEED\_120MN] and [OP\_BLEED\_30MN]. 16895-707-000-RPT-0001 Revision E-BPE. AMEC. October 2011. (E)

**[Ref-4]** EDF/AREVA Task Analysis of Post Fault Claim H2 [OP\_LHSI\_IND\_120MN]. 16895-707-000-RPT-0003 Revision H-BPE. AMEC. October 2012. (E)

**[Ref-5]** EDF/AREVA GDA Task Analysis: Entry into Severe Accident Management Guidelines (OSSA). 16895-707-000-RPT-0006 Revision E-BPE. AMEC. August 2012. (E)

**[Ref-6]** EDF/AREVA Task Analysis of M2 [OP\_EFW/MSRT\_2HLOCAL] and M7. [OP\_SBODG30M]. 16895-707-000-RPT-0004 Revision F-BPE. AMEC. October 2012. (E)

**[Ref-7]** EDF/AREVA GDA Task Analysis: Operator responses to decreasing RCS level (OP\_SIS\_INJ\_80MN\_NCSSL) on the Non Computerised Safety System. 16895-707-000-RPT-0010 Revision G-BPE. AMEC. October 2012. (E)

**[Ref-8]** EDF/AREVA GDA Task Analysis: Steam Generator Tube Rupture Recovery Strategies. 16895-707-000-RPT-0002 Revision I-BPE. AMEC. October 2012. (E)

**[Ref-9]** EDF/AREVA GDA Task Analysis of Post Fault Claims M6 [OP\_FSCD\_30MN\_IH], M8 [OPE\_52] and M19 [OP\_COMBI\_240MN\_LDEP]. 16895-707-000-RPT-0005 Revision D-BPE. AMEC. September 2012. (E)

**[Ref-10]** EDF/AREVA GDA Task Analysis: Primary Circuit Depressurisation in the EOP and the OSSA. 16895-707-000-RPT-0007 Revision D-BPE. AMEC. October 2012. (E)

**[Ref-11]** EDF/AREVA GDA Task Analysis: Operator Responses to Loss of Instrumentation and Control [OP\_EFWS]. 16895-707-000-RPT-0008 Revision D-BPE. AMEC. September 2012. (E)

**[Ref-12]** EDF/AREVA GDA Task Analysis: NCSS Action for OP\_EFWS\_NCSSL, OP\_FB\_120\_MDEP\_NCSSL, OPE\_52\_LOCAL, OP\_SBODG\_LOCAL. 16895-707-000-RPT-0011 Revision D-BPE. AMEC. October 2012. (E)

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 128 /130
		Document ID.No. UKEPR-0002-181 Issue 06

**[Ref-13]** EDF/AREVA GDA Task Analysis: NCSS Action for OP\_BLEED\_30MN\_NCSS. 16895-707-000-RPT-0024 Revision D-BPE. AMEC. August 2012. (E)

**[Ref-14]** EDF/AREVA GDA Task Analysis Summary Report. 16895-707-000-RPT-0025 Revision B-BPE. AMEC. October 2012. (E)

**5.4. DETERMINISTIC SAFETY ANALYSIS**

**5.4.1. Identification and Substantiation of Pre-Fault Claims (Type A and B)**

**5.4.1.1. Dropped Loads**

**[Ref-1]** Identification of Dropped loads and Fuel Handling Human Based Safety Claims- Refueling Machine. PEPS-F DC 135 Revision B. AREVA. July 2012. (E)

**[Ref-2]** Identification of Dropped loads and Fuel Handling Human Based Safety Claims- Polar Crane. PEPS-F DC 134 Revision B. AREVA. June 2012. (E)

**[Ref-3]** Dropped Loads and Fuel Handling: Methodology for the Identification of the Human Based Safety Claims. PEPS-F DC 96 Revision D. AREVA. January 2012. (E)

**5.4.1.2. Heterogeneous Boron Dilution**

**[Ref-1]** Task Analysis Methodology: Analysis of Type A and B Pre-fault Human Errors. 17163-707-000-RPT-0001 Issue 06. AMEC. September 2011. (E)

**[Ref-2]** EDF/AREVA GDA Task Analysis : Method statement and analysis of two example operators claims. 16474/TR/0003 Issue D-BPE. AMEC. May 2012. (E)

**[Ref-3]** EDF/AREVA GDA Human Factors Issue: Heterogeneous Boron Dilution. 16895-707-000-RPT-0014 Revision F-BPE. AMEC. August 2012. (E)

**5.4.2. Identification and Substantiation of Post-Fault Claims (Type C)**

**5.4.2.1. Steam Generator Tube Rupture**

**[Ref-1]** EPR™ UK - GDA - Single Tube Steam Generator Tube Rupture Analysis for the UK. PEPR-F.10.1665 Revision 3. AREVA. September 2012. (E)

**[Ref-2]** EDF/AREVA GDA Task Analysis: Steam Generator Tube Rupture Recovery Strategies. 16895-707-000-RPT-0002 Revision I-BPE. AMEC. October 2012. (E)

**[Ref-3]** Steam Generator Tube Rupture – Mitigation Strategy. PEPR-F DC 38 Revision D. AREVA. October 2012. (E)

**5.4.2.2. Internal Flooding**

**[Ref-1]** Internal Flooding – Bounding Cases: Mitigation Measures Report. ECEIG111647 Revision B. EDF. January 2012. (E)

**[Ref-2]** Internal Flooding. 16895-707-000-RPT-0013 Revision E-BPE. AMEC. September 2012. (E)

**[Ref-3]** UK-EPR-Internal Flooding- Multi-Legged safety case and ALARP consequence assessment analysis. ECEIG121115 Revision B. September 2012. (E)

<b>UK EPR</b>	<b>PRE-CONSTRUCTION SAFETY REPORT</b>	SUB-CHAPTER : 18.1
		PAGE : 129 /130
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	Document ID.No. UKEPR-0002-181 Issue 06

## **6. HUMAN FACTORS PROCESS ASSURANCE**

### **6.1. ROLES, RESPONSIBILITIES AND INTERFACES**

#### **6.1.1. FA3 Initial Reference Design**

##### **6.1.1.3. Operators and Nuclear Operation Department's Representatives**

[Ref-1] ISO. Human-centred design processes for interactive systems. ISO 13407. 1999. (E)

#### **6.1.2. UK EPR Specific Roles, Responsibilities and Interfaces**

[Ref-1] EPR UK-GDA issue HF01- Organisation note and resources identification. ECESN120038 Revision B. EDF. June 2012. (E)

##### **6.1.2.5. PSA specialists**

[Ref-1] Human Factors Engineering Programme Review Model. NUREG 0711 Revision 2. USNRC. February 2004. (E)

[Ref-2] A D Swain. Accident Sequence Evaluation Program Human Reliability Analysis Procedure. NUREG/CR-4772. Sandia National Laboratories. Albuquerque. New Mexico. February 1987. (E)

### **6.3. OVERSIGHT OF SUB-CONTRACTORS**

#### **6.3.1. FA3 Initial Reference Design Work**

[Ref-1] EPR - Organisation de la surveillance des études d'installation et suivi des modifications des données dans la maquette PDMS par bâtiment. [Process for Monitoring of Installation Studies and Tracking of PDMS model data modifications, by Building]. ECEIG070082 Revision A. EDF. June 2007.

This document is only available in French and is provided for information only.

#### **6.3.2. UK EPR specific HF Studies**

[Ref-1] EPR UK-GDA issue HF01- Organisation note and resources identification. ECESN120038 Revision B. EDF. June 2012. (E)

### **6.4. HFE PROCESSES AND DOCUMENTATION**

#### **6.4.1. FA3 Initial Reference Design**

##### **6.4.1.1. Design Quality Plan**

[Ref-1] Approach for integration of human factors in EPR design. ECEF012001 Revision A. EDF. December 2001. (E)

##### **6.4.1.3. Design Specifications**

[Ref-1] Specifications for Nuclear Auxiliary Building. ECEIG0000333 Revision E1. EDF. February 2008. (E)

UK EPR	PRE-CONSTRUCTION SAFETY REPORT	SUB-CHAPTER : 18.1
	CHAPTER 18: HUMAN FACTORS AND OPERATIONAL ASPECTS	PAGE : 130 /130
		Document ID.No. UKEPR-0002-181 Issue 06

[Ref-2] Specifications for Safeguard Auxiliary and Electrical Buildings. ECEIG0000810 Revision C1. EDF. January 2010. (E)

[Ref-3] A Meziere, P Bily. Reactor Building Specification. ECEIG0001089 Revision C1. EDF. September 2009. (E)

ECEIG0001089 Revision C1 is the English translation of ECEIG0001089 Revision C.

[Ref-4] Diesel Building: Specifications of the Diesels Buildings ECEIG0000756 Revision C1. EDF. February 2009. (E)

[Ref-5] Fuel Building Specification. ECEIG99070 Revision B1. EDF. March 2010. (E)

**6.4.1.4. HF Evaluation and Review of Design**

[Ref-1] Human Factors programme for evaluation of the EPR's operating means before the 1st fuel loading. HT54200701446 Version 1.0. EDF. May 2009. (E)

[Ref-2] Approach for integration of Human Factors in EPR design. ECEF012001 Revision A. EDF. December 2001. (E)

**6.4.2. UK EPR Specific HF studies**

**6.4.2.2. HF Issues and Assumptions Management**

[Ref-1] Human Factors Tracking Registers. UKEPR-I-042 Revision 1. EDF/AREVA. November 2012. (E)

**6.5. DESIGN CHANGE CONTROL PROCESSES**

[Ref-1] UK EPR GDA Project - Reference Design Configuration. UKEPR-I-002. EDF/AREVA. (E)

[Ref-2] UK EPR GDA Project - Design Change Procedure. UKEPR-I-003. EDF/AREVA. (E)