| UK EPR | Title: PCSR – Sub-chapter 7.5 – Class 3 Instrumentation and Control Systems<br>**UKEPR-0002-711 Issue 01** |
|---|---|
| Total number of pages: 41 | Page No.: I / V |
| Chapter Pilot: B. WORINGER<br>*Name/Initials* B. Woringer *Date* 30-10-2012 | |
| Approved for EDF by: A. MARECHAL<br>*Name/Initials* A.J.C. Marechal *Date* 31-10-2012 | Approved for AREVA by: G. CRAIG<br>*Name/Initials* G Craig *Date* 31-10-2012 |

**REVISION HISTORY**

| Issue | Description | Date |
|---|---|---|
| 00 | First issue.<br>Note: the RRC-B Safety Automation System (§1), Process Information and Control System (§2), Process Automation System (§3), and Severe Accident I&C System (§4) were previously covered by Sub-chapter 7.4.<br>For clarity, the changes from the previous text in Sub-chapter 7.4 are sidelined in this document as follows:<br>- Minor editorial changes<br>- Clarification of text<br>- Update and addition of references<br>- Update of Safety Function Categorisation and SCC Classification to clearly summarise Category A, B, C and Class 1, 2, 3 for I&C scope<br>- Architecture : Class 1 manual control and indication systems in the MCR and RSS<br>- Role of RRC-A in Defence in Depth Concept and associated allocation<br>- Electrical and functional isolation for interfaces to systems of different safety class<br>- Response times involving network communication achievable | 27.03.11 |
| 01 | Consolidated PCSR update:<br>- References listed under each numbered section or sub-section heading numbered [Ref-1], [Ref-2], [Ref-3], etc<br>- Minor editorial changes<br>- Update and addition of references<br>- Clarification of text and addition of cross-references (§1, §1.0, §1.4.3, §2.0.2.1.1, §2.0.2.1.2, §2.0.2.1.3, §2.4.1, §2.4.3, §2.5, §3.0, §3.3.2, §4.0, §4.4.1, §4.4.3.2, §7.5.4 Figure 1) | 31.10.2012 |

Continued on next page

**REVISION HISTORY (Cont'd)**

| Issue | Description | Date |
|---|---|---|
| 01 cont'd | Consolidated PCSR update:<br>- Justification provided for the end to end response times for the plant bus and terminal bus (§2.3.2) | |

**For information address**:

AREVA NP SAS
Tour AREVA
92084 Paris La Défense Cedex
France

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

## TABLE OF CONTENTS

# SUB-CHAPTER 7.5 – CLASS 3 INSTRUMENTATION AND CONTROL SYSTEMS

## 1. RRC-B SAFETY AUTOMATION SYSTEM (RRC-B SAS)

Note: Refer to the quality plans, system specification reports and overall architecture drawings for more detailed information on the Safety Automation System (SAS), which is also applicable to RRC-B SAS [Ref-1] to [Ref-7].

### 1.0. SAFETY REQUIREMENTS

The Risk Reduction Category B (RRC-B) SAS is subject to the safety requirements applicable to Class 3 I&C systems, due to its management of Category C RRC-B functions (with the exception of functions devoted to the particular Loss Of Offsite Power (LOOP) severe accident scenario, allocated to the Severe Accident I&C system (SA I&C), see section 4 of this sub-chapter).

The requirements are detailed in several documents, which provide all the required information contained within an IEC 61513 compliant system requirements specification, as demonstrated for the SAS in section 1.0 of Sub-chapter 7.4 [Ref-1] and for the PAS in section 3.0 of this sub-chapter [Ref-2].

The RRC-B SAS enables the processing of mostly manual actions, together with the associated monitoring, necessary for the performance of the I&C Functions detailed below.

#### 1.0.1. Safety functions

The RRC-B SAS contributes to the RRC-B functions related to prevention of large releases in the event of a postulated low pressure core melt, with the exception of the LOOP RRC-B sequence. It contributes to the following safety functions:

- primary circuit depressurisation;
- hydrogen control (mitigation);
- containment depressurisation and heat removal;
- radiological source term monitoring.

It should be noted that a significant number of RRC-B functions are passive without requiring I&C management.

With regard to the safety analysis, the RRC-B SAS performs RRC-B Category C seismic classified I&C Functions.

The RRC-B SAS will not be allocated any Category A or Category B I&C Functions.

## 1.0.2. Design requirements

The RRC-B SAS must meet the requirements detailed below. These requirements must be met for all the I&C Safety Features managed by the RRC-B SAS.

### 1.0.2.1. Requirements resulting from the functional classifications

#### *1.0.2.1.1. Functional classification of the system*

The RRC-B SAS must be safety-classified, in accordance with the classification indicated in Sub-chapter 3.2.

#### *1.0.2.1.2. Single failure criterion*

The single failure criterion does not apply to the RRC-B SAS.

#### *1.0.2.1.3. Emergency power supplies*

The electrical power supply for the RRC-B SAS equipment must be backed-up by the Emergency Diesel Generators. Moreover, the power supply must be uninterruptible, guaranteeing the power supply even during switching between normal power and diesel power (i.e. it must ensure that the RRC-B SAS I&C Functions can continue without interruption).

In addition, the electrical power supply for the RRC-B SAS equipment must be backed-up by the Ultimate Diesel Generators. For that reason, the RRC-B SAS equipment is located in electrical divisions 1 and 4.

#### *1.0.2.1.4. Qualification under operating conditions*

The RRC-B SAS equipment must remain operational in severe accident conditions, and must therefore meet the qualification requirements defined in Sub-chapter 3.6.

Moreover, the RRC-B SAS equipment must be operational in both normal and extreme environmental conditions applicable to the I&C equipment rooms in which it is located. These conditions are defined in section 1 of Sub-chapter 9.4.

#### *1.0.2.1.5. Electrical and I&C classifications*

The electrical and I&C classification of the RRC-B SAS is consistent with the classification principles given in Sub-chapter 3.2.

#### *1.0.2.1.6. Seismic classification*

The RRC-B SAS meets the seismic requirements defined in Sub-chapter 3.2.

#### *1.0.2.1.7. Periodic testing*

The I&C Functions managed by the RRC-B SAS must be tested periodically (as defined in section 1 of Sub-chapter 3.2). The RRC-B SAS must be designed to allow periodic tests.

#### *1.0.2.1.8. Additional requirements*

Not applicable.

#### 1.0.2.2. Hazards

The RRC-B SAS is not subject to requirements regarding internal hazards.

Protection against external hazards for the RRC-B SAS system concerns only seismic phenomena and is defined consistent with the principles in Sub-chapter 3.2.

### 1.0.3. Tests

After installation, the RRC-B SAS must be subject to pre-operational testing to verify that it conforms to the system performance required by the design.

The requirements for periodic testing are set out in section 1.0.2.1.7 of this sub-chapter.

## 1.1. ROLE

A Severe Accident (RRC-B) is an abnormal event which leads to the meltdown of the core within the Reactor Pressure Vessel (RPV) and is likely to cause a potential release of radiation due to an RPV failure. The management of a Severe Accident is primarily accomplished by RRC-B SAS equipment. Combined with the passive safety systems dedicated to Severe Accident scenarios, and with local manual commands, it provides the necessary mitigation path to limit discharges of radioactivity to the environment.

## 1.2. FUNCTIONS PERFORMED

The I&C Functions processed by the RRC-B SAS have the same features as other Standard I&C automation systems:

- **Data processing:** acquisition and/or conditioning (example: monitoring of core outlet temperature, radioactivity monitoring…);
- **Processing of application calculations:** most I&C Functions are manual (example : manual opening of the SA relief valve in electrical division 4);
- **Processing of monitoring signals:** Processing of status and fault check-backs, generation of alarms and status indications.

## 1.3. DESIGN BASIS

### 1.3.1. Availability requirements

The main availability requirements for the RRC-B SAS are linked to the reliability and the maintainability of the system i.e.:

- to limit the loss of the RRC-B SAS due to failure of one of its components (mainly by component redundancy);
- to facilitate the maintenance and repair of the RRC-B SAS to minimise downtime.

### 1.3.2. Performance requirements

The RRC-B SAS is subject to specific performance requirements:

- Response time requirements:
  - maximum time from the variation of an input signal (analogue or digital) to transmission to an output interface;
  - maximum time from the receipt of a manual command to its transmission to an output interface.

These global criteria are applied to the RRC-B SAS as follows:

- for a manual command, see section 2.3.2 of this sub-chapter;
- for an automatic command: not applicable.

The RRC-B SAS must contribute to fulfilling the global criteria described above and in section 2.3.2 of this sub-chapter

In particular, the two acquisition, processing and transmission actions performed by the RRC-B SAS must be compatible with the required total response time (including Safety Information and Control System (MCS [SICS]), Process Information and Control System (MCP [PICS]), RRC-B SAS and level 0 components and systems).

- Sizing requirements:
  - static sizing includes actuators, sensors and I&C Functions that the RRC-B SAS supports;
  - dynamic sizing includes sampling and processing times, taking into account the way in which the I&C Functions are processed (periodic or event-triggered).

### 1.3.3. Environmental requirements

The ambient conditions that the RRC-B SAS must tolerate are linked to the temperature and relative humidity of the rooms housing this equipment. The environmental characteristics are defined in Sub-chapter 9.4, for normal and extreme conditions.

### 1.3.4. Human-machine interface requirements

The RRC-B SAS must interface with an engineering Human-Machine Interface (HMI) to enable safe, effective and error-free commissioning, maintenance, periodic testing and configuration of the RRC-B SAS.

The operational HMI for the RRC-B SAS is provided by the level 2 I&C systems (see section 1.1 of Sub-chapter 7.2).

## 1.4. ARCHITECTURE

### 1.4.1. Structure and composition

The structure and composition of the RRC-B SAS are dictated by the functional requirements. This set of requirements affects the allocation of I&C processing tasks to the various components within the RRC-B SAS.

These functional requirements relate to the following:

- The functional classification of the processing (all RRC-B SAS I&C Functions are Category C);
- The electrical division (together with the processing cabinet, and associated actuators and sensors) : RRC-B SAS I&C Functions are allocated to electrical divisions 1 and 4;
- The processing performance requirements (response times, propagation times, accuracy);
- The processing groupings/exclusions which require certain processes to be grouped (due to the requirement to simultaneously shut down all these processes in the event of malfunction of part of the I&C system that manages them), or conversely, that certain processing groups need to be managed by different input/output boards.

In addition, the RRC-B SAS structure takes into account the segmentation of the process being controlled, dictated by the number, geographic location and type of actuator and sensor interfaces to be managed.

Unlike the Class 2 Plant SAS, the RRC-B SAS does not have any dedicated SAS Bus interface, but only its Class 3 Plant bus interface.

### 1.4.2. Installation

The RRC-B SAS equipment is installed in the I&C cabinet rooms of divisions 1 and 4 in the safeguard buildings.

The RRC-B SAS cabinets are positioned considering:

- consistency with the location and division of the actuators and the sensors to be managed;
- available space; and

- consistency with the electrical supplies of the electrical divisions.

### 1.4.3. Interfaces with other I&C systems

The RRC-B SAS exchanges information with the following:

- the HMI, MCS [SICS] in the MCR and MCP [PICS] in both the MCR and RSS, related to plant operation by the operator;
- the PAS, related to the plant automation management;
- the instrumentation process associated with measurement and data acquisition;
- the switchgear units (electrical boards) and the control devices (electro-positioners, etc.) that are associated with actuator controls;
- the “external” systems (I&C cabinets for the diesels, etc.), associated with the units automation management.

Concerning the RRC-B SAS interfaces: The RRC-B SAS I&C Functions have the characteristics, in accordance with the defence in depth concept, of being autonomous in relation to other I&C systems at level 1 of the I&C architecture. This means that these I&C Functions do not depend on information coming from other systems and the interfaces are limited in number.

## 1.5. OPERATING CONFIGURATIONS

The configuration of the RRC-B SAS (from the hardware and functional points of view) is independent of the plant situation. Processing allocation depends only on functional criteria and on the allocation principles of the I&C system. The configuration of the RRC-B SAS is, from this point of view, constant.

The RRC-B SAS configuration is based on the principle that, in the event of malfunction of an active CPU, the system switches to a redundant standby unit. This principle applies to all the redundant RRC-B SAS boards (CPU boards and communication management boards).

## 1.6. TECHNOLOGY

The equipment used to implement the RRC-B SAS is the digital I&C system based on SPPA-T2000 [Ref-1].

## 1.7. POWER SUPPLY

Within each of divisions 1 and 4, the I&C cabinets of the RRC-B SAS are supplied by a dual power supply via independent AC/DC converters and DC/DC converters. One power supply is provided by a 400V AC supply and the other by a 220V DC supply with appropriate converters.

The voltage required by the cabinets will be regulated internally in dedicated power supply cabinets. These power supply cabinets are situated in the same rooms as the I&C cabinets.

The description of the power supply distribution of the NI is given in Sub-chapter 8.3.

## 1.8. PROVISIONS FOR PERIODIC TESTING

All I&C Functions are subject to periodic testing.

The safety function test will allow the verification of the whole control channel, from the sensor, or from the MCP [PICS]/MCS [SICS], via RRC-B SAS, up to the change of state of the actuator.

However, if reconfiguration of the relevant actuator cannot be carried out (for example, during plant operation), provisions are taken for blocking the control signals during the test, so that the actuator control line can be tested without physically controlling it.

# 2. PROCESS INFORMATION AND CONTROL SYSTEM (MCP [PICS])

Note: Refer to the quality plans, system specification reports and overall architecture drawings for more detailed information on the Process Information and Control System (MCP [PICS]) [Ref-1] to [Ref-7].

## 2.0. SAFETY REQUIREMENTS

The MCP [PICS] is subject to the safety requirements applicable to Class 3 I&C systems.

### 2.0.1. Safety functions

The way the MCP [PICS] contributes to the I&C Functions is described in Sub-chapter 7.1. With regard to safety, the MCP [PICS] provides the operators with information and command facilities necessary to operate and monitor the plant in normal (PCC-1) operating conditions (conditions within the limits of the normal functioning of the installation) and also in RRC-A and RRC-B situations. The MCP [PICS] is required to be designed to support Category C I&C Functions.

The MCP [PICS] is also the preferred means of control to ensure optimised operation of the installation in PCC-2 to PCC-4 conditions (see Chapter 14 for more details).

### 2.0.2. Design requirements

#### 2.0.2.1. Requirements resulting from functional classification

##### *2.0.2.1.1. Functional classification of the system*

The MCP [PICS] is a Class 3 system and supports Category C and non-categorised operating and monitoring I&C Functions according to the classification principles described in Sub-chapter 3.2. The MCP [PICS] is a Class 3 I&C system.

The MCP [PICS] is the preferred means of control to ensure optimised operation of the installation in PCC-2 to PCC-4 conditions. In addition to its Class 3 requirements, the following requirements apply to the MCP [PICS]:

- operator workstation equipment and the architecture of the computerised Human-Machine Interface in the Main Control Room (MCR) must meet requirements applicable to Class 2 systems;
- the corresponding software must meet related qualification requirements proposed by the designer in the RCC-E (implementation of those parts of IEC 62138 standard for Class 3 computer-based systems) [Ref-1];
- systems must be implemented (outside the MCP [PICS]) for the detection of failures of the MCP [PICS] processing units and associated network links, and these systems must meet the requirements applicable to Class 2 systems.

#### *2.0.2.1.2. Single failure criterion*

The single failure criterion is not required for the Class 3 I&C Safety Features of the MCP [PICS]. Due to the application of Class 2 requirements to operator workstation equipment and to the architecture of the computerised Human-Machine Interface in the control room, the single failure criterion must be met by the architecture of this sub-set of MCP [PICS] equipment.

#### *2.0.2.1.3. Emergency power supply*

Due to the MCP [PICS] being Class 3, a requirement for a backed-up power supply of the MCP [PICS] equipment is defined on a case-by-case basis.

Due to the application of Class 2 architecture and design requirements for electrical back-up to the operator workstation equipment and to the architecture of the computerised Human-Machine Interface in the control room, the power supply of the associated equipment must, at least, be backed-up by the Emergency Diesel Generators. In addition, this power supply must be of an "uninterruptible" type in all possible operating modes and corresponding transients.

#### *2.0.2.1.4. Qualification under operating conditions*

The MCP [PICS] equipment must be qualified according to its safety class, and must in consequence meet the qualification requirements (integrity, availability, etc.) defined in Sub-chapter 3.6, under normal and extreme environmental conditions to which they are subjected in carrying out their task (see section 2.3.3 of this sub-chapter).

#### *2.0.2.1.5. Electrical and I&C classifications*

The electrical and I&C classification of the MCP [PICS] is consistent with the classification principles given in Sub-chapter 3.2.

#### *2.0.2.1.6. Seismic classification*

MCP [PICS] system meets the seismic requirements defined in Sub-chapter 3.2.

#### *2.0.2.1.7. Periodic testing*

MCP [PICS] equipment is subject to periodic tests.

### 2.0.2.2. Hazards

The MCP [PICS] must be protected against common cause failures that can result from internal or external hazards by meeting requirements defined in Sub-chapter 3.1 (external and internal hazards).

## 2.0.3. Tests

### 2.0.3.1. Pre-operational tests

The MCP [PICS] must be subject to pre-operational tests to check that, after installation, the system performance conforms to the design requirements.

#### 2.0.3.2. Monitoring during operation

Class 2 systems implemented to detect and annunciate potential failures of the MCP [PICS] processing units enable monitoring of the correct operation of the MCP [PICS] processing units in the control room.

#### 2.0.3.3. Periodic tests

All I&C Functions must be subject to periodic testing. The equipment must be designed so that specific periodic tests can be performed.

## 2.1. ROLE

The Process Information and Control System (MCP [PICS]) is the I&C system that supports the computerised means for command and monitoring of the installation. It includes:

- the operator workstations and the Plant Overview Panel (POP) installed in the MCR;
- the operator workstations installed in the Remote Shutdown Station (RSS);
- the operator workstation installed in the Technical Support Centre (TSC) for supervision;
- the basic operator workstations (with fewer screens) that can be installed in addition to the computerised operating means in particular plant situations (e.g. commissioning) or for specific activities (e.g. maintenance).

In addition, the MCP [PICS] records significant events that occur in the plant and provide the interface with the non real-time applications (also called level 3 applications) such as the application for document assistance.

The main function of the MCP [PICS] is to provide the operators with controls, information and operating guides that are fully appropriate to their tasks, in any plant situation. As this function entails an interaction with operators, the MCP [PICS] Human-Machine Interface must comply with ergonomic criteria taking into account the cognitive and physiological aptitudes of the operators.

## 2.2. FUNCTIONS PERFORMED

In order to meet the objective described in the previous section, the MCP [PICS] must provide the following features:

- Display functions:
    - o displaying graphical images including representing data from sensors, operating guides, alarm sheets, technical sheets and lists;
    - o navigation through different images;
    - o designation of the item with which the operator must interact;
    - o updating images (colour, shape of objects etc.) according to the process state;

- visualisation and plotting curves;
- printing of various images or lists.

- Instrumentation and Control functions:
  - sending commands to actuators via the I&C systems;
  - displaying command feedback;
  - allowing the presentation of data to the operator.
- Alarm functions:
  - warning the operators as soon as an alarm occurs;
  - managing the lists of alarms;
  - allowing access to alarm sheets.
- Processing functions:
  - managing databases;
  - initiating processing in the event of a change of state;
  - elaborating information if needed (situations, alarms, synthetic information etc.).
- Interface functions:
  - retrieving and filtering data from the process via the automation level;
  - sending commands to the process via the automation level.
- Archiving function:
  - archiving digital and analogue data;
  - retrieving archived data;
- Administrative and maintenance functions:
  - providing help for maintenance;
  - managing the introduction of data into operation;
  - providing help for analysis (e.g. analysis of workstation access etc.);
  - ensuring security tasks (e.g. the management of workstation access etc.);
  - self monitoring.

These features help ensure that the results of the Human Factors programme described in Sub-chapter 18.1 are made available to the shift team. To complement these features, special attention is paid to the design of the interface and the working environment as detailed in section 2.3.3 below.

## 2.3. DESIGN BASIS

### 2.3.1. Availability requirements

The main objectives for MCP [PICS] architecture are availability, flexibility and maintainability. In particular, this means that the MCP [PICS] architecture must be sufficiently flexible and redundant to:

- prevent most losses of MCP [PICS] due to the failure of one item of equipment;
- allow redistribution of the working area (screens, operating workstations etc.) when some equipment (screen, computer etc...) is unavailable;
- facilitate maintenance and repair to minimise the period of unavailability of the MCP [PICS];
- allow connection of additional components (for example additional operator workstations) during specific phases (e.g. commissioning, maintenance).

### 2.3.2. Performance requirements

The MCP [PICS] is subject to particular performance requirements:

- Response time requirements: these requirements are intended to ensure that the MCP [PICS] is able to provide the necessary level of information whatever the plant situation;
- Global criteria concerning the following:
    - maximum permissible time between a variation occurring at level 0 (sensor level) and the update of the corresponding information on screen;
    - maximum permissible time between an operator action and the transmission of the corresponding command to the actuator;
    - time necessary for requested information to reach the operator.
- These global requirements are taken into account in the design of the MCP [PICS] by specifying:
    - for a manual command (from the action of the operator to transmission to level 1) taking into account the HMI response time, the accuracy of the transmitted value and the transit time;
    - for feedback from a manual command (from level 1 output to screen update) taking into account the response time for the visualisation display, the accuracy of the displayed value and the transit time;

- for the visualisation of a sensor value (from level 1 output to the screen update) taking into account the response time for the visualisation display, the accuracy of the displayed value and the transit time.

- Sizing requirements:

  - static sizing specification includes the number of actuators, sensors etc. that the MCP [PICS] must manage and the number of images, animated objects, procedures pages, alarms sheet etc. that must be supported by the computerised operating system;

  - dynamic sizing specification includes specification of the number of state changes or analogue variations that the MCP [PICS] must be able to process within a fixed interval of time.

Values for the different criteria listed above will be defined in detailed studies as for FA3. They depend mainly on ergonomic criteria (e.g. response time for information refreshment or command feedback; type of information and its organisation for static sizing), or on functional studies. An analysis of the FA3 studies and tests shows that the design derived time responses are considerably more pessimistic than those determined by the testing performed. It presents arguments for the acceptability of the results that have been obtained and argues that the equipment to be used for the UK EPR can be expected to produce more acceptable results. It is noted that the numerical criteria for the time responses are not safety related limits but are average response time targets [Ref-1].

### 2.3.3. Environmental requirements

The environmental requirements depend largely on the location of the different equipment items (MCR or RSS or I&C cabinet rooms).

They are divided into two categories:

- the environmental conditions that the equipment must withstand. This includes temperature and relative humidity of the equipment room;

- the impact of the equipment on local environmental conditions. This category includes noise level and dissipated heat.

For display equipment, some particular environmental conditions, such as lighting, must be considered from an ergonomic point of view. The provisions that must be made are determined as part of the Human Factors approach (see Sub-chapter 18.1 for a description of the Human Factors programme, particularly with regard to definition of requirements for lighting and other environmental conditions).

### 2.3.4. Human-machine interface requirements

The MCP [PICS] must interface with an engineering HMI to enable safe, effective and error-free commissioning, maintenance, periodic testing and configuration of the MCP [PICS].

With regard to the Human Factors approach, the MCP [PICS] plays two roles:

- the MCP [PICS] must have the functionality necessary to implement the results of the Human Factor approach (e.g. treatment and type of supported data, organisation of data, layout of information, means of navigation, alarm system, operating help mechanisms etc.);
- the MCP [PICS] must provide a working environment for the operators with an interface that meets the requirement of the state-of-the-art ergonomic criteria (organisation of the different means of control in the MCR, workstation layout, dialogue methods, communications methods etc).

These requirements are included in the Human Factors programme described in Sub-chapter 18.1.

The operational HMI for the MCP [PICS] is provided by the level 2 I&C systems (see section 1.1 of Sub-chapter 7.2).

## 2.4. ARCHITECTURE

### 2.4.1. Structure and composition

To accomplish its objective, the MCP [PICS] includes the following resources (software and/or hardware):

- graphical interfaces for the Human-Machine Interface;
- network interfaces for data exchange;
- real time data bases (process and elaborated data, and their attributes, Human-Machine Interface data);
- archiving and printing facilities;
- operating systems;
- application software.

These resources are used by the following equipment:

- control workstations in the MCR and in the RSS;
- monitoring workstations in the MCR and in the TSC;
- a POP incorporating large screens in the MCR;
- basic operator workstations for use during specific phases (e.g. commissioning) or specific tasks;
- a set of computers, either associated with the workstations or, if required, centralised and installed in the I&C cabinet rooms (divisions 1 and 4);

- equipment allowing printing;
- equipment allowing archiving;
- interfaces with engineering tools;
- interfaces with other non real time (level 3) applications;
- networks for exchange of data between MCP [PICS] and level 1 or 3 systems.

Operator workstations consist of standardised screens refreshed by processing units depending on the content of databases and pointing and data input devices (mice, keyboards, etc).

Operator workstations, whether they operate in control mode or monitoring mode, are based on similar equipment and provide similar functionality. Any monitoring workstation installed in the MCR or in the RSS can be configured on-line to become a control workstation to allow a reallocation of operator workstation in the event of total loss of an operator workstation in control mode. This flexibility is controlled by procedures.

The number of workstations, their detailed composition (e.g. number of screens), their organisation in the MCR, RSS or TSC, is determined by the Human Factors Engineering programme (see Sub-chapter 18.1).

The POP is considered as an integral part of the MCP [PICS]: therefore, it is subject to the same functional classification (i.e. Category C/non-categorised) and could be considered as an operator workstation configured in monitoring mode. Therefore simultaneous failure of the POP and MCP [PICS] must be considered, especially in the MCS [SICS] design.

The I&C Functions supported by the MCP [PICS] are organised within the equipment listed above in order to satisfy safety and availability requirements:

- MCP [PICS] and MCS [SICS] components are chosen to be sufficiently diverse to minimise the risk of common cause failure (i.e. the MCS [SICS] is conventional and the MCP [PICS] is a digital system). This measure is reinforced by appropriate equipment installation measures (see Sub-chapter 7.7);
- the processing equipment needed to control and monitor the plant from the RSS workstations is installed in I&C cabinet rooms of divisions 1 and 4, outside the MCR (in a different fire compartment to the MCR) so that it cannot be lost simultaneously with the MCR;
- MCP [PICS] architecture is fault-tolerant, i.e. the design takes account of criteria for redundancy and independence so that probable failures will not result in a loss of HMI functions.

### 2.4.2. Installation

The MCP [PICS] equipment is typically installed as follows:

- In the main control room (MCR):
  - operator workstations in control mode;
  - operator workstations in monitoring mode;

- basic operator workstations with a reduced number of screens, some of which may be temporary (e.g. for initial start-up);
- POP;
- printing devices.

- In the remote shutdown station (RSS):
  - operator workstations in control mode (when the RSS is active, or otherwise in monitoring mode );
  - one basic operator workstation configured in monitoring mode;
  - printing devices.
- In the technical support centre (TSC):
  - operator workstation in monitoring mode;
  - printing devices.
- In the I&C cabinet rooms of division 1 and 4 of the safeguard buildings:
  - processor units (PU);
  - server units (SU);
  - RAID system (Division 4 only).

### 2.4.3. Interfaces with other I&C systems

The MCP [PICS] has three types of interfaces with other I&C systems:

- the interface with the automation level (Protection System (RPR [PS])[1] / SAS / PAS / (Reactor Control, Surveillance and Limitation system, RCSL) / (Severe Accident I&C system, SA I&C)[2]);
- the interface with the engineering and maintenance tools (of MCP [PICS]);
- the interface with non real time (level 3) applications.

[1] The connection to the RPR [PS] is unidirectional from the RPR [PS] to the MCP [PICS] and is a Class 3 networked interface.

[2] The SA I&C provides status data to MCP [PICS] via a network link.

## 2.5. OPERATING CONFIGURATIONS

From the I&C standpoint, the various modes of operation of the MCP [PICS] are as follows:

- The standard configuration of the MCP [PICS] is:
  - all operator workstations of the MCR, whether they are in control mode or monitoring mode, are working;
  - the POP is operational;
  - the workstations of the RSS are in monitoring mode;
  - the TSC operator workstation is not operational except in a situation where a support team is needed. In this situation, the TSC operator workstation is in monitoring mode.
- Non-critical failure of MCP [PICS] equipment. In this situation, a part of the MCP [PICS] has failed but sufficient means are still available to allow a redistribution of the operation I&C Functions to allow continued use of the MCP [PICS] to control and monitor the plant. Typical situations are as follows:
  - loss of non-graphical equipment: the redistribution of the process resources or interface resources is in most cases done automatically by the system (e.g. through redundancy mechanisms) and it does not affect significantly the operator tasks;
  - loss of a screen of an operator workstation: as the screens of an operator workstation are standardised, the operator can redistribute tasks from the lost screen to the remaining screens;
  - loss of an operator workstation in control mode: a workstation in monitoring mode can be configured to control mode to replace the loss;
  - loss of a part of the POP: the POP is divided into several areas in the same way that an operator workstation has several screens. This allows redistribution of the display of the POP using the remaining areas in the event of failure of one of the large screens making up the POP;
  - loss of the POP: All information shown on the POP is also available from the operator workstations, therefore in this situation the operators would use these to continue operations. Loss of the POP does not lead to the loss of the MCP [PICS].

In addition to these arrangements, special attention is paid to maintenance and repair tasks to reduce the time needed to replace or repair the component that has failed.

- Unavailability of the MCP [PICS] In the event of accidental loss of MCP [PICS] or a shutdown of the MCP [PICS] scheduled for maintenance purposes, control is transferred to the MCS [SICS]. The transfer is controlled by procedures. For the I&C, those procedures stipulate particular actions to prevent spurious control signals being generated by the MCP [PICS] which are taken into account by the process [Ref-1] [Ref-2]. The MCP [PICS] is monitored by the SAS. The SAS displays the MCP [PICS] status on the PSIS. When control is passed to MCS [SICS] it sends a message to the SAS to block the MCP [PICS] outputs.

- Unavailability of the MCR: in the event of loss of the MCR due to an internal hazard (e.g. fire), the equipment of the MCS [SICS] and of the MCP [PICS] located in the MCR is no longer available. In this situation, the shift team uses the control system situated in the RSS. As for the previous configuration, particular actions must be taken to prevent spurious control signals being generated from the MCR. The configuration of the MCP [PICS] is as follows:

    - RSS workstations are operational and configured in control mode;

    - All command means of the MCP [PICS] in the MCR are isolated to avoid spurious commands; see section 1.5.3 of Sub-chapter 7.2 for details.

The way in which the various MCP [PICS] operator workstations are used to control or supervise the unit is detailed in Sub-chapter 18.1.

The different configurations (particularly different configurations arising due to unavailability of the MCP [PICS] and non-critical failure of one of the components) are determined by setting the minimum equipment required to operate the plant with the MCP [PICS] (minimum number of screens needed to operate the plant from an operator workstation, minimum number of control and supervision workstations to operate the plant etc.). These limits depend on the way in which the different items of equipment are used and are therefore mainly determined by the Human Factors engineering programme (see Sub-chapter 18.1).

## 2.6. TECHNOLOGY

The equipment used to implement the MCP [PICS] is the digital Operating and Monitoring system OM690, which is part of the SPPA-T2000 platform.

## 2.7. POWER SUPPLY

The processing part of the MCP [PICS] (which is located outside the MCR) is electrically powered by divisions 1 and 4 so that the loss of one of these two power sources does not lead to the total loss of MCP [PICS]. The power supply for the operator workstations in the MCR is from divisions 1 to 4 so that the power distribution in the MCR would minimise the impact on the MCR equipment if there was a loss of electrical power from one division.

A description of the power distribution system in the NI is given in Sub-chapter 8.3.

## 2.8. PROVISIONS FOR PERIODIC TESTING

All MCP [PICS] equipment is subject to periodic testing.

# 3. PROCESS AUTOMATION SYSTEM (PAS)

Note: Refer to the quality plans, system specification reports and overall architecture drawings for more detailed information on the Process Automation System [Ref-1] to [Ref-12].

## 3.0. SAFETY REQUIREMENTS

The PAS is subject to safety requirements applicable to Class 3 I&C systems, due to its management of Category C I&C Functions.

The requirements are detailed in several documents, which provide all the required information contained within an IEC 61513 compliant system requirements specification [Ref-1].

The PAS processes automatic and manual actions and the related monitoring required to fulfil the I&C Functions described below.

### 3.0.1. Safety functions

The PAS is an operational system that participates in the three main safety functions defined in Sub-chapter 3.2. Due to this operational aspect, PAS I&C Safety Features fulfil Category C I&C Functions.

### 3.0.2. Design requirements

The PAS must fulfil the requirements described below. These requirements must be met for all the automatic I&C Safety Features managed by the PAS (including the part of the PACS functions processed by the PAS equipment according to section 1.4 of Sub-chapter 7.2).

#### 3.0.2.1. Requirements resulting from functional classification

##### *3.0.2.1.1. Functional classification of the system*

The PAS is required to be safety classified, in accordance with the classification principles in Sub-chapter 3.2.

##### *3.0.2.1.2. Single failure criterion*

The single failure criterion does not apply to the PAS.

Independence and physical separation must be provided when:

- the PAS is used to reduce the consequences of internal or external hazards. In this situation its operation must not be affected (in an unacceptable manner) by the hazard.

#### *3.0.2.1.3. Emergency power supply*

The requirement for emergency power supplies to PAS equipment is defined on a case-by-case basis. If required, the power supply must be backed-up by the Emergency Diesel Generators. In these cases, the power supply must be "uninterruptible" to ensure continuation of the supply during the switchover from normal to diesel power supplies.

The PAS is required to be powered from the same division or section that is supplying the process that the PAS is controlling.

#### *3.0.2.1.4. Qualification under operating conditions*

The PAS equipment must remain operational in post-accident conditions. It must therefore meet the qualification requirements defined in Sub-chapter 3.6.

In addition, the equipment must remain operational in normal and extreme environmental conditions occurring in the plant rooms in which it is installed. These conditions are defined in Sub-chapter 9.4.

#### *3.0.2.1.5. Electrical and I&C classification*

The electrical and I&C classification of the PAS is consistent with the classification principles given in Sub-chapter 3.2.

#### *3.0.2.1.6. Seismic classification*

The PAS equipment meets the seismic requirements defined in Sub-chapter 3.2.

#### *3.0.2.1.7. Periodic testing*

The I&C Functions managed by the PAS must be tested periodically (as defined in section 1 of Sub-chapter 3.2). The PAS must be designed to allow periodic tests.

#### *3.0.2.1.8. Additional requirements*

Not applicable.

### 3.0.2.2. Hazards

The PAS system manages automatic control and monitoring I&C Functions designed to reduce the consequences of internal and external hazards. These I&C Functions must remain operational following a hazard, and thus must not be affected (to an unacceptable extent) by the hazard itself or by its consequences. For these I&C Functions, an analysis is performed on a case-by-case basis to define the measures to be implemented (redundancy, separation, independence) to protect the PAS equipment against hazards.

## 3.0.3. Tests

The PAS system must be subjected to pre-operational tests to check that, after installation, the system performance complies with design requirements.

The requirements associated with the periodic tests are given in section 3.0.2.1.7.

## 3.1. ROLE

The role of the PAS is to manage the required Category C non-seismically qualified and non-categorised I&C Functions of the nuclear and conventional islands and the site (see section 3.0.1).

## 3.2. FUNCTIONS PERFORMED

The PAS carries out the following I&C Functions:

- **data processing:** acquisition, conditioning and transmission;
- **processing of application calculations:** regulations, generating individual and grouped commands (simultaneous or sequential), hierarchical organisation of the priorities of commands, generating diverse information to be sent to other instrumentation and control units, etc.
- **survey processing:** processing of state and default reports, alarms and signals elaboration.

Refer to section 1 of Sub-chapter 7.2 for details of how Risk Reduction Category A (RRC-A) I&C Functions are allocated in PAS.

## 3.3. DESIGN BASIS

### 3.3.1. Availability requirements

The main requirements on PAS availability are linked to reliability and maintainability, and are summarised as follows:

- To reduce the probability of losses of the PAS due to the failure of one of its components (i.e. by providing redundancy of components);
- To facilitate maintenance and repair to minimise the duration of unavailability of the PAS.

### 3.3.2. Performance requirements

The PAS is subject to specific performance requirements (see section 3 of Sub-chapter 7.1 for more detail of where these will be defined) and is subject to the following performance requirements:

- Response time requirements:
    - Maximum allowable time between the variation of an input signal (digital or analogue) and the transmission to the output interface;

- Maximum allowable time between the receipt of a manual command and the transmission to the output interface.

These global criteria are adapted to the PAS as follows:

- for a manual command, see section 2.3.2;
- for an automatic command:
  - acquisition of a digital input, processing of the digital command, and transmission to an output interface;
  - acquisition of an analogue input signal, calculation of a digital or analogue command, and transmission to an output interface.

The PAS conforms with the global criteria described above and with those of section 2.3.2.

In particular, the transmission and processing I&C Functions performed by the PAS must conform to the total response time requirements (including the exchanges between MCP [PICS] in both the MCR and RSS, PAS and level 0).

Sizing requirements:

- Static sizing requirements define the number of input/outputs (actuators, sensors, etc.) that the PAS has to manage;
- Dynamic sizing requirements define the processing times, taking into account the program execution types (periodic or event-driven) that the PAS must manage.

### 3.3.3. Environmental requirements

The environmental conditions that the PAS equipment must withstand relate to the temperature and relative humidity in the rooms where the equipment is located. These environmental conditions (normal and extreme) are described in section 1 of Sub-chapter 9.4.

### 3.3.4. Human-machine interface requirements

The PAS must interface with an engineering HMI to enable safe, effective and error-free commissioning, maintenance, periodic testing and configuration of the PAS.

The operational HMI for the PAS is provided by the level 2 I&C systems (see section 1.1 of Sub-chapter 7.2).

## 3.4. ARCHITECTURE

### 3.4.1. Structure and composition

The structure and the composition of the PAS are dictated by functional requirements. These requirements govern the allocation of the treatment of control commands in the different entities of the PAS.

The functional requirements deal with:

- the functional classification of the processing I&C Functions;
- the electrical division or train (which corresponds with that of the process, actuators and sensors, to be managed);
- the type of processing to be performed (which may condition the choice of the type of input/output cards for example);
- the performance required of the processing function (response time, propagation time, accuracy);
- the grouping/exclusions of processing required. Certain processing I&C Functions are grouped (in relation to requirements due to a simultaneous loss of processing I&C Functions during a malfunction of the part of the I&C system that controls them). Conversely, there may be a requirement for certain processing I&C Functions to be controlled by different PAS hardware units (to preserve operability of a group of processing I&C Functions despite loss of certain others due to a malfunction).

Furthermore, the structure of the PAS takes into account the segmentation of the process control dictated by the number, location and the type of interfaces of actuators and sensors to be managed.

For a given safety function, different combinations are possible e.g.:

- 1 x 100 %: One mechanical train, with its associated I&C, is necessary to fulfil the safety function;
- 4 x 50 %: Two out of four mechanical trains, with their associated I&C, are necessary to fulfil the safety function;
- 2 x 100 %: One out of two mechanical trains, with its associated I&C, is necessary to fulfil the safety function.

In order to prevent an internal failure having an impact on more than one mechanical train, each mechanical train is controlled by a sub-system of the PAS located in the same division or section as the mechanical train.

### 3.4.2. Installation

The equipment, which manages the I&C Functions of the PAS, is distributed within the four divisions of the nuclear island and in the two sections of the conventional island and site. It is installed in the I&C cabinets of divisions 1 to 4 of the safeguard buildings, in the I&C cabinets of the two sections of the conventional island, and in the I&C cabinets of the site buildings.

The PAS equipment is located:

- in correspondence with the location of the division or section of the systems (actuators and sensors) managed;
- in accordance with the space available;
- in correspondence with the power supply division or section.

### 3.4.3. Interfaces with other I&C systems

The PAS exchanges information with the following:

- Process instrumentation: exchanges linked to the acquisition of measurements and states;
- The HMI: MCP [PICS]/RSS, and MCS [SICS]: exchanges linked with operator control;
- The RCSL, RPR [PS], and SAS: exchanges* associated with the management of plant process control;
- Electrical cells (electrical boards) and the control systems (electro-positioners etc.): exchanges linked to actuator control;
- "External" systems (turbine I&C cabinets, etc.): exchanges linked to the management of the plant process control.

* Note that the communication from higher class systems is managed by the higher class system and is usually unidirectional (from the higher class to the lower). See section 1.4.3 of Sub-chapter 7.3 for the description of the interfaces from the RPR [PS] to lower class systems.

## 3.5. OPERATING CONFIGURATIONS

The configuration (hardware and functional aspects) of the PAS is independent of the plant state. Processing allocation only depends on functional criteria and the processing allocation principles of the I&C system. The configuration of the PAS is, from this point of view, constant.

The configuration of the PAS is subject to the following principle: in the event of a malfunction of an active board, the system switches automatically to the redundant standby board. This principle applies to any redundant card of the PAS (CPU cards and communication management cards).

## 3.6. TECHNOLOGY

The equipment used to implement the PAS is the digital I&C system based on SPPA-T2000.

## 3.7. POWER SUPPLY

Within each division, the I&C cabinets of the PAS are supplied by a dual power supply, via independent AC/DC converters and DC/DC converters. One power supply is provided by a 400V AC supply and the other by a 220V DC supply with appropriate converters.

Each mechanical train is controlled by a sub-system of the PAS that is located and electrically supplied by the same electrical division as the mechanical train.

The adjustment to the voltage required by the PAS cabinets will be made internally to the cabinet supplying them with power. The supply cabinets are located in the same room as the PAS cabinets.

The description of the power supply distribution of the NI is given in Sub-chapter 8.3.

## 3.8. PROVISIONS FOR PERIODIC TESTING

Periodic tests are required for all classified I&C Functions.

The testing of a function must allow verification of the complete command channel, from the sensor (automatic command), or from the MCP [PICS] via the PAS (manual command), up to the change of state of the actuator.

However, if effecting an actuator change of state is not feasible (e.g. during operation of the plant) provisions are taken to block the command signals while the test is in progress, in order to test the line of command of the actuator without effecting the command.

# 4. SEVERE ACCIDENT I&C SYSTEM (SA I&C)

Note: Refer to the quality plans, system specification reports and overall architecture drawings for more detailed information on the SA I&C system [Ref-1] to [Ref-7].

## 4.0. SAFETY REQUIREMENTS

The SA I&C is subject to safety requirements applicable to Class 3 I&C systems, due to its management of Category C I&C Functions.

The requirements are detailed in several documents, which provide all the required information contained within an IEC 61513 compliant system requirements specification as demonstrated for the RPR [PS] in section 1.0 of Sub-chapter 7.3.

### 4.0.1. Safety functions

The Severe Accident (SA) I&C system participates in the following main safety function:

- Limiting the radioactive releases at the site boundary to an acceptable level and maintaining the integrity of the primary and secondary systems.

The SA I&C system performs the Severe Accident I&C Functions (RRC-B functions) needed in the event of a total loss of power (Loss of Off-site Power (LOOP) and loss of Emergency Diesel Generators and loss of Ultimate Diesel Generators).

### 4.0.2. Design requirements

#### 4.0.2.1. Requirements resulting from functional classification

##### *4.0.2.1.1. Functional classification of the system*

The Severe Accident I&C system must be classified according to the principles specified in Sub-chapter 3.2.

##### *4.0.2.1.2. Single failure criterion*

Not applicable.

##### *4.0.2.1.3. Emergency power supply*

To compensate for the total loss of power scenario, the SA I&C system will be supplied by redundant Uninterruptible Power Supply (UPS) systems using battery-backed systems with a 12 hour capacity.

##### *4.0.2.1.4. Qualification under operating conditions*

The SA I&C components performing a Category C I&C Function must be qualified to remain functional under post-accident and severe accident conditions.

The relevant requirements for components (integrity, operability, functional capacity etc.) are given in Sub-chapter 3.6.

#### *4.0.2.1.5. Electrical and I&C classification*

The electrical and I&C classification of the system is consistent with the classification principles given in Sub-chapter 3.2.

#### *4.0.2.1.6. Seismic classification*

The SA I&C system meets the seismic requirements defined in Sub-chapter 3.2.

#### *4.0.2.1.7. Periodic testing*

The I&C Functions managed by the SA I&C must be tested periodically (as defined in section 1 of Sub-chapter 3.2). The SA I&C must be designed to allow periodic tests.

#### 4.0.2.2. Hazards

The SA I&C system is not subject to requirements regarding internal hazards.

Protection against external hazards for the SA I&C system concerns only seismic phenomena and is defined consistent with the principles in Sub-chapter 3.2.

### 4.0.3. Tests

Pre-operational tests must prove the adequacy of the design and the performance of the SA I&C system.

The requirements associated with the periodic tests are given in section 4.0.2.1.7.

## 4.1. ROLE

A Severe Accident (RRC-B) is an abnormal event which leads to the meltdown of the core within the Reactor Pressure Vessel (RPV) and is likely to cause a potential release of radiation due to a PRV failure. The management of a Severe Accident is primarily accomplished by the RRC-B SAS (see section 1 of this sub-chapter).

The SA I&C system provides the necessary commands and information in the event of a Severe Accident coupled with or due to a total loss of power (Loss of Off-site Power (LOOP) and loss of Emergency Diesel Generators and loss of Ultimate Diesel Generators).

The SA I&C system, combined with the passive safety systems dedicated to Severe Accident scenarios, provides the necessary mitigation path to limit discharges of radioactivity to the environment.

## 4.2. FUNCTIONS PERFORMED

The SA I&C system is designed to implement the following functions:

- Manual opening of the Severe Accident relief valves;
- Monitoring of the core outlet temperature;
- Monitoring of the corium location;
- Annulus Ventilation System (EDE [AVS]) iodine train heater regulation;
- Hydrogen monitoring;
- Containment pressure monitoring;
- Radioactivity monitoring.

## 4.3. DESIGN BASIS

### 4.3.1. Environmental requirements

#### 4.3.1.1. Normal conditions

The equipment must be able to operate in the ambient conditions set out in section 1 of Sub-chapter 9.4.

#### 4.3.1.2. Accident conditions

The components of the SA I&C system performing RRC-B I&C Functions must remain operational in post-accident and severe accident conditions.

This applies mainly to components subject to accident conditions in the reactor building (e.g. sensors and transmitters). The components located in the I&C rooms of the safeguard buildings operate in all plant conditions, including accidents, under the same environmental conditions.

### 4.3.2. Human-machine interface requirements

The SA I&C must interface with an engineering HMI to enable safe, effective and error-free commissioning, maintenance, periodic testing and configuration of the SA I&C.

The operational HMI for the SA I&C is provided by the level 2 I&C systems (see section 1.1 of Sub-chapter 7.2).

## 4.4. ARCHITECTURE

### 4.4.1. Structure and composition

The SA I&C system comprises two Severe Accident Units (SAUs)

Since it is the only type of unit of the system, the SAU performs all the tasks necessary for the fulfilment of the SA I&C I&C Functions:

- Sensor acquisition;
- Data processing;
- Actuator control.

The SA I&C system also manages the acquisition of manual commands from the dedicated SA panel located within the MCS [SICS] and the transmission of analogue and digital information to the SA panel for display, when this panel is activated by the operator.

There are two SAUs, one is installed in division 1 and one is installed in division 4. They are network connected. In addition to the two SAUs there are dedicated units for the interface to the MCP [PICS] in the service unit.

The input and output modules of the SA I&C are designed to ensure the required electrical separation [Ref-1].

The architecture of the SA I&C system is given in Section 7.5.4 – Figure 1.

### 4.4.2. Installation

The SAUs of the SA I&C system are installed within the I&C cabinet rooms of safeguard buildings 1 and 4.

### 4.4.3. Interface with other I&C systems

#### 4.4.3.1. Inputs

The SA I&C system receives:

- From the instrumentation system:
  - Analogue values of sensor measurements.
- From the dedicated SA panel located with the MCS [SICS]:
  - Manual commands.
- From the electrical switchgear:
  - Test check-backs for periodic test purposes.

#### 4.4.3.2. Output

The SA I&C system provides:

- The switchgear with:
  - Commands.
- The AVS Heater Control switch with:
  - Closed loop control signals.
- The dedicated severe accident panel of the MCS [SICS] with:
  - Analogue and digital sensor measurements;
  - Processed analogue values; and
  - Alarms.
- the MCP [PICS] (via a network link) with:
  - Information and alarms to be displayed and logged.

## 4.5. TECHNOLOGY

The equipment used to implement the SA I&C system is the AREVA NP TELEPERM XS (TXS) digital I&C platform.

It is described in section 1.4 of Sub-chapter 7.3 and in section 1 of Sub-chapter 7.7.

## 4.6. OPERATING CONFIGURATIONS

The SA I&C system comprises a set of computerised TXS units. The operating modes of the computerised TXS units are described in section 1 of Sub-chapter 7.3.

## 4.7. POWER SUPPLY

The I&C cabinets of the SA I&C system are supplied by UPS systems. The UPS systems are fed from 2 busses:

- A 220V DC power supply backed-up by 2 hour batteries; and
- A 400V AC power supply backed-up by 12 hour batteries.

The power supplies from these busses are further converted to +24V DC power and supplied via a double +24V DC in-feed to the cabinets enabling the SA I&C system to operate for 12 hours in the event of a total loss of power.

Design measures ensure that the power supply delivers the required electrical separation.

The NI power supply is described in Sub-chapter 8.3.

## 4.8. PROVISION FOR MAINTENANCE AND I&C TESTS

### 4.8.1. Maintenance

For maintenance purposes (software downloading, parameter modification, component replacement), the maintenance team is able to act on the SA I&C system without impairing the operability of the system.

It is possible to switch off the unit, by means of the Service Unit and hardware release keys, in order to perform maintenance, internal tests or diagnosis.

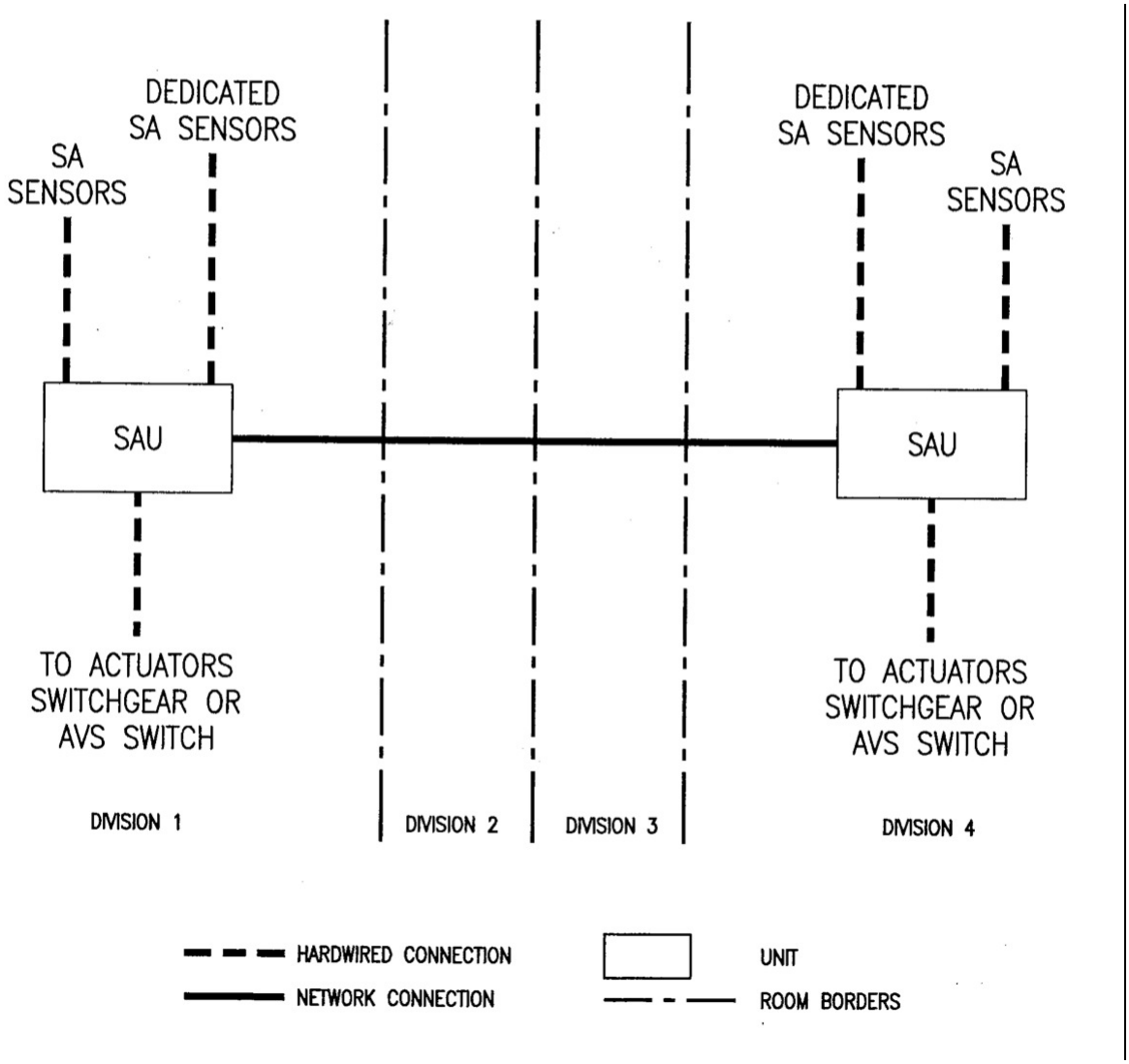
### 4.8.2. Test

The self-test features of the TXS hardware and the use of the Service Unit for the periodic testing fulfil the periodic test requirements.

Periodic testing is performed at a frequency determined by the probabilistic safety requirements for the equipment that processes the severe accident I&C Functions. The various types of test are performed in an overlapping manner in such a way that the instrumentation, the processing equipment, the actuator control and the interfaces between all such parts are all tested.

## SECTION 7.5.4 - FIGURE 1

**SA I&C system architecture**



# SUB-CHAPTER 7.5 – 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. RRC-B SAFETY AUTOMATION SYSTEM (RRC-B SAS)

**[Ref-1]** Project Development Plan relating to FA3 Standard I&C. NLF-F-DC 11 Revision C. AREVA. June 2007. (E)

**[Ref-2]** Quality plan for engineering of FA3 standard I&C based on SPPA-T2000. NLF-F DC 82 Revision C. AREVA. April 2008. (E)

**[Ref-3]** 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-4]** System Qualification Program. NLF-F DC 14 Revision D. AREVA. March 2009. (E)

**[Ref-5]** Kristel. System specification file (DSS). SY710 Version 6.0. Siemens. March 2009. (E)

**[Ref-6]** J Latour. Overall Architecture Drawing. NLN-F DC 91 Revision A. AREVA. December 2009. (E)

NLN-F DC 91 Revision A is the English translation of NLF-F DC 10 Revision E.

**[Ref-7]** Application Software Test program. NLF-F-DC 89 Revision C. AREVA. December 2009. (E)

### 1.0. SAFETY REQUIREMENTS

**[Ref-1]** UKEPR: SAS IEC 61513 System Requirements Specification (SRS) Equivalence. ECECC121435 Revision A. EDF. August 2012. (E)

**[Ref-2]** SRS Equivalence Justification Note for PAS and PACS. ECECC121609 Revision A. EDF. August 2010. (E)

### 1.6. TECHNOLOGY

**[Ref-1]** Basis of Safety Case of SPPA-T2000. PEL-F DC 13 Revision A. AREVA. June 2012. (E)

# 2. PROCESS INFORMATION AND CONTROL SYSTEM (MCP [PICS])

**[Ref-1]** Project Development Plan relating to FA3 Standard I&C. NLF-F-DC 11 Revision C. AREVA. June 2007. (E)

**[Ref-2]** Quality plan for engineering of FA3 standard I&C based on SPPA-T2000. NLF-F DC 82 Revision C. AREVA. April 2008. (E)

**[Ref-3]** System Qualification Program. NLF-F DC 14 Revision D. AREVA. March 2009. (E)

**[Ref-4]** Kristel. System specification file (DSS). SY710 Version 6.0. Siemens. March 2009. (E)

**[Ref-5]** J Latour. Overall Architecture Drawing. NLN-F DC 91 Revision A. AREVA. December 2009. (E)

NLN-F DC 91 Revision A is the English translation of NLF-F DC 10 Revision E.

**[Ref-6]** Specification for the KIC [PICS] Plant System: Instrumentation and Control Systems for Computerised Control. ECECC040729 Revision A1. EDF. June 2010. (E)

**[Ref-7]** Process Information and Control System (KIC [PICS]) Part 5: Control and Instrumentation System EPR FA3 (Stage 2). ECECC080097 Revision B1. EDF. June 2010. (E)

## 2.0. SAFETY REQUIREMENTS

### 2.0.2. Design requirements

#### 2.0.2.1. Requirements resulting from functional classification

##### *2.0.2.1.1. Functional classification of the system*

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

## 2.3. DESIGN BASIS

### 2.3.2. Performance Requirements

**[Ref-1]** Justification of time response end to end on Terminal Bus Plant Bus. ECECC111368 Revision B. EDF. August 2012**.** (E)

## 2.5. OPERATING CONFIGURATIONS

**[Ref-1]** System Specification for KSC Plant System: Safety Information and Control System and layout of Main Control Room, Remote Shutdown Station and Emergency Technical Centre. ECECC060019 Revision A1. EDF. July 2010. (E)

**[Ref-2]** C Botta. System Design Manual - Main Control Room (KSC [MCR]), Part 5: Control and Instrumentation System (KSC [MCR]) EPR FA3 (Stage 2). ECECC070760 Revision B1. EDF. November 2009. (E)

# 3. PROCESS AUTOMATION SYSTEM (PAS)

**[Ref-1]** Project Development Plan relating to FA3 Standard I&C. NLF-F-DC 11 Revision C. AREVA. June 2007. (E)

**[Ref-2]** 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-3]** Quality plan for engineering of FA3 standard I&C based on SPPA-T2000. NLF-F DC 82 Revision C. AREVA. April 2008. (E)

**[Ref-4]** System Qualification Program. NLF-F DC 14 Revision D. AREVA. March 2009. (E)

**[Ref-5]** Kristel. System specification file (DSS). SY710 Version 6.0. Siemens. March 2009. (E)

**[Ref-6]** J Latour. Overall Architecture Drawing. NLN-F DC 91 Revision A. AREVA. December 2009. (E)

NLN-F DC 91 Revision A is the English translation of NLF-F DC 10 Revision E.

**[Ref-7]** Application Software Test program. NLF-F-DC 89 Revision C. AREVA. December 2009. (E)

**[Ref-8]** E Marotte. KC Plant System. - Level 1 Instrumentation and Control Equipment Document Part 1 - DSE History. ECECC070931 Revision B1. EDF. September 2009. (E).

**[Ref-9]** E. Marotte, G. Saoutieff. KC System DES (Plant System File) - Part 2: KC. System operations. ECECC070539 Revision B1. EDF. September 2009. (E).

**[Ref-10]** E. Marotte, G. Saoutieff. KC Plant System File – Part 3: Designing KC. system. ECECC070902 Revision B1. EDF. September 2009. (E)

**[Ref-11]** E. Marotte, G. Saoutieff. KC Plant System File – Part 4: KC system Mechanical Diagrams. ECECC070935 Revision B1. EDF. September 2009. (E)

**[Ref-12]** E. Marotte, G. Saoutieff. KC Plant System File - Part 5: KC System I&C. ECECC070903 Revision B1. EDF. September 2009. (E)

### 3.0. SAFETY REQUIREMENTS

**[Ref-1]** SRS Equivalence Justification Note for PAS and PACS. ECECC121609 Revision A. EDF. August 2010. (E)

## 4. SEVERE ACCIDENT I&C SYSTEM (SA I&C)

**[Ref-1]** TELEPERM XS – System Overview. ANP:G-49 V1.0. AREVA. 2006. (E)

**[Ref-2]** TXS I&C Systems Verification and Validation Plan. PELV-F DC 28 Revision A. AREVA. June 2012. (E)

**[Ref-3]** SA I&C - Detail Specification File. NLE-F DC 106 Revision C. AREVA. August 2009. (E)

**[Ref-4]** SA I&C - Functional Diagrams. NLE-F DC 169 Revision C. AREVA. April 2009.

**[Ref-5]** TELEPERM XS Engineering Procedure Calculation of Response Time and Accuracy of TELEPERM XS channels. NLE-F DM 10014 Revision C. AREVA. September 2010. (E)

**[Ref-6]** TELEPERM XS Engineering Procedure - Methodology for RAMS Studies. NLE-F DM 10032 Revision A. AREVA. June 2010. (E)

**[Ref-7]** PS (incl. RPI sw) / RCSL / SA I&C / PIPS TELEPERM XS I&C System Engineering Quality Plan. PEL-F DC 7 Revision A. AREVA. June 2012. (E)

### 4.4. ARCHITECTURE

#### 4.4.1. Structure and composition

**[Ref-1]** TELEPERM XS based systems. Concept for Electrical Separation. NLE-F DC 249 Revision E. AREVA. January 2011. (E)