SUB-CHAPTER Q.4 HUMAN MACHINE INTERFACE SYSTEMS

0.0 SAFETY REQUIREMENTS

0.1 SAFETY FUNCTIONS

The human-machine interface (HMI) systems must provide the operators with all the facilities they need to monitor and manage the Unit in all circumstances.

The main HMI systems are centralised in the Main Control Room (MCR).

The process information and control system (PICS) is the main interface and, when available, is used by the operators in all situations of the Unit.

The safety information and control system (SICS) is used by the operators in the MCR when the PICS is not available.

When the MCR is not available (for instance, in the event of a fire), an operational interface sited in the Remote Shutdown Station (RSS) is used to manage and monitor the Unit and bring it to a safe state.

0.2 PUBLISHED REGULATIONS

The Technical Guidelines (Chapter C.2) specify the following in relation to the HMI:

Chapter G3 “Design of Instrumentation and Controls” addresses use of the PICS to manage the Unit during an accident and use of the remote shutdown station if the main control room is unavailable.

0.3 REQUIREMENTS FOR SAFETY STUDIES

The requirements for the safety studies for the MCR, the RSS and the TSC are given in the RCC_E standards.

The safety requirements cover:

- the way in which safety information must be presented,
- features of the architecture for the emergency HMI,
- location, environment and protection,
- spatial layout,
- information and control systems (information, controls, coding, alarms, procedures),

- the control and monitoring devices used in the computerised and conventional workstations, and

- communication facilities.

1.0 HMI EQUIPMENT

1.1 MAIN CONTROL ROOM (MCR)

The Unit is managed and monitored in all situations from the MCR, assuming it is available. Management includes commissioning, maintenance, shutdown for refuelling, operation at full power and during accidents. In addition, the MCR has facilities for communication with the outside.

The MCR must remain available if there is an earthquake; MCR equipment required to ensure safety must operate during an earthquake (i.e. the SICS). Other areas may be non-operational, but must not prevent the MCR being used, or jeopardise installations with a safety function.

If the MCR is lost owing to fire, the consequences (spurious level-2 order issued) are restricted to PCC1 events (this defines the scope of situations covered by management from the RSS).

The HMIs used in the MCR are:

- the PICS (process information and control system) – for further details on the requirements of the PICS, refer to Chapter G.4.

- the SICS (safety information and control system) - for further details on the requirements of the SICS, refer to Chapter G.3.

- the Plant Overview Panel, giving an overview of the Unit.

- controls specifically for F1A commands.

1.1.1 PICS workstations

There are four full PICS workstations in the MCR, configured in control or monitoring mode depending on the composition of the operations team. Each workstation has five screens.

Each workstation has an additional processor with a sixth screen. This is not connected to the process and is used to access Level-3 computer applications.

A cut-down workstation with four screens enables others working in the MCR (see Chapter Q.3.1.2.3) to access process information.

The workstation used by each operator gives the ability to manage and monitor the entire Unit under all circumstances (except, of course, when the PICS is unavailable) via the PICS screens. It presents the operational information the operator requires in an appropriate form, so that there is complete awareness of the status of the Unit and the process before decisions are taken or actions initiated.

Non-dedicated Screens

The screens are in no way dedicated to any particular display. This means that any information may be displayed on any screen, and that any screen may be used to start a separate dialog at any given moment.

Functions of the PICS

The PICS has the following fundamental control and information functions:

- relaying digital and analogue information from the process,
- managing all the Unit actuators that can be controlled individually by commands from the MCR,
- displaying the progress and status of processes initiated by commands,
- controlling the I&C functions (automatic sequences, control loops, inputting settings, switching between automatic and manual modes, setting parameters and clearing memory) and displaying the corresponding action logs,
- annunciating and displaying alarms for functions and equipment that impact directly on the control of the process,
- tuning parameters at specific stages, where the tuning relates to the status of the process (if not, the maintenance service does the tuning),
- providing information on the availability and administrative status of actuators and sensors, and
- displaying alarms when equipment necessary to control the process fails, or when events occur that require special attention from the operator or require him to take action manually.

Summary information:

- Information on the state, availability and administrative status of mechanical and electrical systems and sub-systems.
- The means to review malfunctions and failures in the various equipment items controlled by the operators, and the means to plan the future course of the process and the effect of the planned action. These means are provided to pinpoint the failures in the I&C equipment, sensors and actuators that affect the control of the process (via the data sheets).

Information log:

Log display (showing time line, log records of digital information, and manual and automatic actions).

Aids to operation:

- for alarms, displays showing the potential cause, the expected consequences and the potential corrective measures (in the form of alarm sheets),

- displays showing the actions to take in the event of an incident or accident (as an emergency operating procedure), and

- displays showing the actions to take to change the state of the Unit or systems (as procedures), where the actions are not automated.

Documentation function:

- Copies of procedures and other material can be printed from the screen.

Functions to assist in operation

- Access to Level-3 data such as the administrative status of equipment.

Control of access to PICS functions

Access to some operations, including controlling actuators individually and resetting alarms, may be restricted by administration settings at the workstation (password). A particular workstation may be designated either an operational workstation, or a supervisory workstation.

Only authorised personnel may change this assignment (password).

Organisation and composition of the PICS displays

Both the operator's task and the Unit's operational regime (normal or accident) determine how the PICS displays are organised.

There are two main categories of display: process views and instruction views (see Chapter Q.3.2.2.2).

In addition to these two categories, there are particular views designed to meet the requirements of the operations teams. They are:

- the view associated with status diagnostics,

- views breaking down summary information and showing how the summary has been prepared,

- overall views , including general information about the Unit and its parameters. They are used to obtain quick status reports on the state of the Unit during a shift or when the crew changes over, and

- views specifically for the Supervisor, summarising information about the Unit.

This approach will be finalised as the FHF program described in Chapter Q.2 is carried out.

Functions of the supervisor workstation

The supervisor workstation is fundamentally identical to that of the operator, with the same PICS screens. Operation of the unit is possible, but this is password protected. The supervisor workstation may be used to back up the other workstations.

Functions of the MOW (Minimal Operator Workstations)

These workstations have the same functions as a normal operator workstation, but with one screen less. They are used by staff who need to work temporarily in the MCR (see Chapter Q.3 1.2.3).

1.1.2 Emergency control area SICS

The emergency control area has the means to control and monitor the plant systems when the operator workstations in the MCR are not available. In these circumstances, the SICS is the HMI used. It enables the two operators, the supervisor and the safety engineer to manage and monitor the Unit.

In order to achieve a controlled state, the F1A functions may require operator action after the first thirty minutes following a PCC event, so the relevant information and controls will also be available in this area.

The SICS is a conventional control and monitoring facility with a panel display containing buttons, indicator lights, alarm windows and registers, etc.

The operator can carry out the following functions from the SICS:

- monitor and manage the station in a stable power state if the PICS is not available for a short period under normal conditions,

- shut down and maintain the station in a safe state, if the PICS is unavailable for a longer period under normal conditions,

- monitor and implement appropriate operational management functions following accidents, so that the station is brought to and maintained in a safe state when the PICS is not available in a situation defined as PCC-2 to 4, and

- initiate measures to fight fires in the nuclear island when the PICS is not available, for PCC-2 to 4 events.

  the SICS may also be used as a source of specific information to broaden the range of that provided by the PICS, and in particular to help assess the safety of the Unit.

The main features of the SICS are as follows:

- the operational methods provided to control and monitor the power station are essentially restricted to the class F1 functions used for operational management during PCC-2 to PCC-4 events,

- the SICS is designed so that it integrates the controls and information in a way that is ergonomically optimal – the operator has no need to refer to other information sources (such as the Plant Overview Panel) to obtain the information he needs for the task,

- the event log is restricted to the accessible log (24 or 72 hours, depending on the accident analysis rules and what the procedures require if an accident occurs), and

- all the controls and information are directed towards ensuring safety for the transition to a safe state during PCC-2 to PCC-4 events (following a safe path).

Further features of the SICS are given in Chapter G.3.

1.1.3 Plant Overview Panel

The Plant Overview Panel (POP) presents the overall state of the Unit in large format. Assuming the PICS can provide the information, the POP is used for all Unit states.

The POP is used:

- to coordinate the operations teams,
- to provide a common reference, and
- to provide information quickly on the Unit's state.

It presents information selected so that the state of the Unit may be determined.

It displays views showing the status of the main actuators and the main parameters such as temperatures, power ratings, frequency, etc., shown either as graphs or as instantaneous values.

The POP presents large-format images projected onto four screens (retro- or video-projection).

The dialog is accessible from the operator workstations. The operators select which views are presented.

Note that, because the POP interfaces to the PICS computer system, it can also display all the views available from the operator workstations.

The content of the views will be finalised based on the Human Factors (HF) program,.

The synoptic views must be visible and readable from all MCR workstations.

1.1.4 F1A controls

Conventional means for issuing F1A manual commands will be installed in the MCR.

1.2 REMOTE SHUTDOWN STATION (RSS)

If the working environment deteriorates because an accident makes the MCR uninhabitable (fire, gas, smoke, etc.) the room is evacuated to that housing the Remote Shutdown Station (RSS).

The function of the RSS is to control the Unit when the MCR is unavailable, but when there is no other failure or accident, apart from a possible loss of the external power supply.

The RSS area is a temporary work area. Its area is smaller than that occupied by the PICS in the MCR.

1.2.1 Scope

The RSS enables the Unit to be monitored and managed during all PCC-1 situations.

It includes the instrumentation and controls required to bring and maintain the reactor to a safe state. In particular, it is designed to enable the reactor:

- to be quickly brought to the hot shutdown state and to be kept in that state, and

- to be subsequently brought to cold shutdown and to be maintained it in that state by using appropriate procedures and by carrying out operations local-to-plant if controls are not available from the RSS. (Since the HMI in the RSS is similar to that used by the computerised workstations in the MCR, there should, however, be less need to carry out operations locally, compared with previous plant series where the Remote Shutdown Panels used conventional technology.)

When operations are managed from the RSS, the external electrical supply may not be available and the power may thus be derived from the diesel generators supplying the emergency switchboards.

1.2.2 The HMI in the RSS

The RSS has two operator workstations supplied by Divisions 3 and 4 respectively, and one additional workstation supplied by Division 1. These three operator workstations are installed in the same area.

The control and supervision functions are earthquake-classified (see Chapter G.2).

Each operator workstation in the RSS has four screens (instead of the five screens in the computerised workstations in the MCR). The additional workstation has only two screens. It is configurable only in supervisory mode and enables the Operating Manager / Safety Engineer to monitor the state of the Unit without interrupting the two operators. The workstation may be shared by the Operating Manager / Safety Engineer and the supervisor as dictated by the operational requirements.

The workstations in the RSS have the same functionality as those in the MCR. Additionally, the means of communication is the same as that in the MCR.

The equipment for detecting and fighting fires complies with the ETC-F, 2005 version.

The RSS has no Plant Overview Panel.

The installation and operating principles (switching between the MCR and the RSS in particular) are discussed in Chapter G.2.

1.3 LOCAL CONTROLS AND INDICATIONS

If controls and indications are installed local-to-plant, outside the MCR, they will take the form either of:

- a conventional panel (with push buttons, indicator lights, etc.); or
- a computerised interface.

1.4 TECHNICAL SUPPORT CENTRE (TSC)

The TSC is used for operational management after an accident. It provides information and communication facilities to the team of experts supporting and advising operating personnel.

The TSC has a workstation identical to the supervisor workstation in the MCR. All the information held in the PICS is also available on the screens in the TSC. In addition, all the documentation is accessible.

1.5 OTHER LOCATIONS

Computerised workstations connected to the PICS and configured in supervisory mode may be installed outside the MCR to supply information to members of the operations team located outside the MCR (those isolating equipment, watchmen, etc.). Such workstations will be installed appropriate locations (watchmen's premises, room for managing work permits, etc.).

2.0 WORKING ENVIRONMENT REQUIREMENTS

The detailed specification for the operation team's working environment must comply with relevant ergonomic requirements. Based on the current status of the detailed review, those requirements are summarised below. They will be defined in more detail during the EPR detailed design stage, which will include a joint ergonomic and architectural study to define and optimise the layout and the environment of the operational locations.

2.1 MECHANICAL PROPERTIES AND DIMENSIONS FOR THE WORKING ENVIRONMENT

The preliminary designs for the MCR and other locations where the HMI is installed follow basic layout requirements for presenting information on a screen and on conventional control panels.

These requirements are based on specific parameters for visual perception (the minimum angle for reading information on screens and on conventional control panels; determination of a primary field of view per operator; typical sizes of standard equipment such as screens, conventional indicators and control tiles).

2.2 ACOUSTIC ENVIRONMENT

The acoustic environment and the maximum sound level in the MCR and the RSS are specified so that:

- the process monitoring, process control and associated activities may be carried out in comfort,
- there is good communication between members of the operations team, and
- audible signals are heard clearly.

This requires a sufficiently low average background sound level, good acoustics in the MCR, and appropriate auditory signals.

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

- choosing the location and monitoring the design and implementation of equipment that could transmit sound via its structure,
- 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 is to create a closed volume isolated from the main civil-engineering structure by intermediate elastic supports that damp the vibrations transmitted by neighbouring installations.

2.3 LIGHTING FOR HMI ROOMS AND WORK AREAS

The lighting in the MCR must provide optimal working conditions for the operations team. This requires:

- providing a lighting level suitable for the 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 lighting in the MCR, the RSS and the TSC is backed up by at least two trains. An emergency uninterruptible power supply (accumulator batteries) guarantees a minimum lighting level.

Some lighting in the MCR is also supplied from the power sources provided for managing severe accidents (see Chapter H.3.5.4).

2.4 ENVIRONMENTAL CONDITIONS IN THE MCR AND ADJOINING ROOMS

The environmental conditions in the MCR and its adjoining rooms are set out in the Tables in Chapter I.4.1.