XA9846513

THE COMPUTER-AIDED OPERATION OF THE N4 SERIES

G. GUESNIER, J.P. BOUARD
Electricité de France, Engineering and Construction Division
Basic Design Department
Villeurbanne, France

Abstract

Designed at the beginning of the eighties, subject of many months of evaluation and validation between 1987 and 1996 on a full scope simulator, the computer-based control room and the fully integrated computerised I&C system of the N4 series are now under operation. Today, Chooz NPP unit 1 and 2 are connected to the French grid (since 1996) and the unit of Civaux 1 is in the final phase of commissioning tests. Start up of the last (Civaux 2) is scheduled in summer 1998. The commissioning hitches inherent to any innovation have been resolved, the safety authority has granted operating licenses. This short but significant operating time associated to the commissioning phases have generated a first positive experience feedback which has consolidated the decision made by EDF in the design of this project, as well on the MMI point of view as on the I&C architecture one. Finally it has led to the decision taken by EDF, its European partners in the EURs (European Utilities Requirements) and the German utilities partnering the EPR project (European Pressurised Reactor), to choose this control-room concept for future plants.

1. INTRODUCTION

In the early eighties, EDF decided to start designing a new control-room concept and the architecture of a fully integrated computerised I&C system, with the overall objective of reducing human factor-related risks by changing the control-room design, and so improving the quality of operation.

2. OBJECTIVES AND MAIN OPTIONS

The objectives chosen from the outset of the project were as follows:

- to reduce the amount of information presented to the operator, and to make it better and more relevant,

- to develop processing modes for the generation and presentation of information, and alarm processing in particular, in order to facilitate the understanding of this information and adapting it to the operating context,

- to strengthen the exchange of information between the operating and maintenance structures, so that operating procedures took better account of the actions carried out by the plant maintenance teams,

- to search for a single interface for all operating conditions,

- to develop processing modes to assist operation, and to achieve the optimum integration of these modes in the operating procedures.

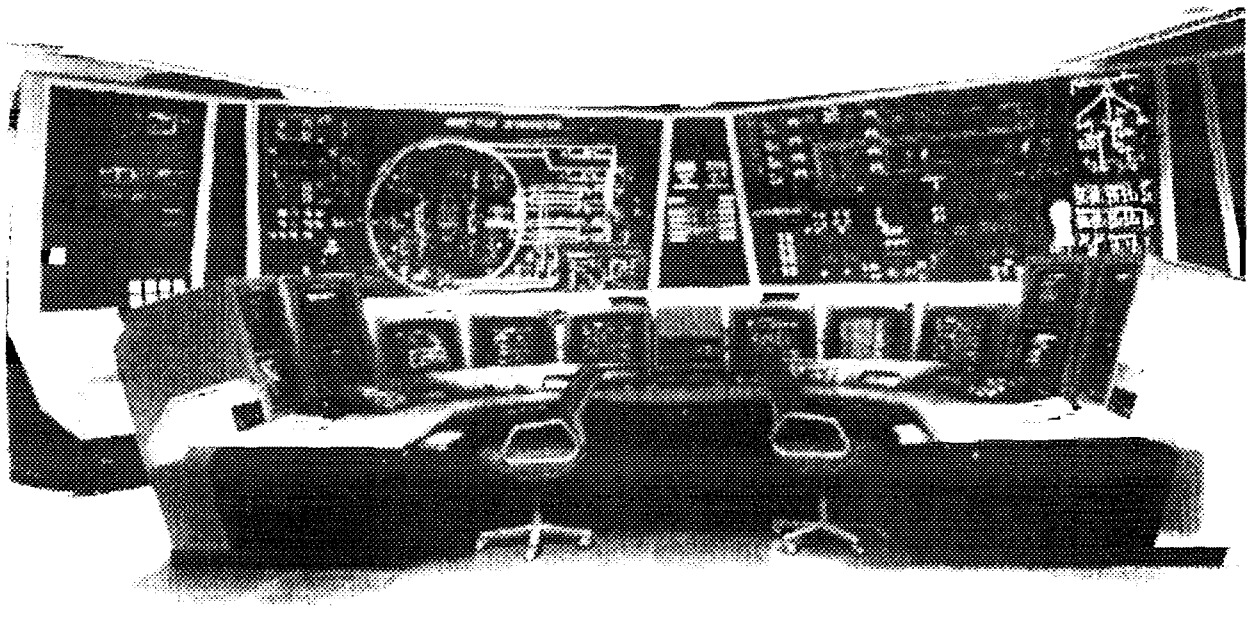
To realise these objectives, the following main options were adopted:

- all information from the plant would undergo systematic validation processing,

- computing facilities would be used to present information and issue orders: firstly in order to place a wide range of information at the operator's disposal ; secondly to associate controls and information relating to the same operating action, whether this action concerns equipment start-up or shutdown, adjustments, procedure application or alarm-sheet processing.

Because of this last option, a seated operating position was chosen.

3. MAIN FEATURES OF THE CONTROL ROOM



Control room of 1450 MW plants (N4 Series)

Operation from the control room is carried out from workstations which are computerised for all plant condition categories. This choice provides the following advantages:

- to have the same operating facilities available in all conditions (the concept of a "normal" operating workstation and an "accident" operating workstation was rejected),

- to provide the operator with high-power information and control equipment, in order to ensure high-quality information and presentation,

- to avoid a mixture of conventional and computerised equipment (a hybrid control room) ; besides the drawback of heterogeneous presentation of equipment, this design makes it difficult to draw a clear line between the computerised and conventional controls.

Four workstations are installed in the control room. They are identical and standardised: two are operating workstations for the two operators ; the other two are observation workstations (actions on the process are locked) for the use of the technical supervisor and the shift operations manager or safety engineer.

In addition, to provide the operating team with a rapid plant overview and supplement the fragmented view supplied by the display screens, a large wall-mounted mimic panel, whose moving elements (indicators, positions) can be read from the operator workstations, was installed in the control room.

All this equipment, supplemented by reprographics, printing and telecoms equipment and by several surveillance systems (fire protection, access control, etc.), is necessary and adequate for plant operation.

A computer link with the lockout management system for maintenance jobs informs the operators, on their screens, of the "lockout" status of equipment.

These options privileged the "human factor-ergonomy" aspect : they required the implementation of computing equipment for which full unavailability had to be considered in economically acceptable conditions, given the current level of technology.

In addition to the provisions described above, the design also included diversified operating equipment in the form of a panel with conventional operating equipment which is independent from the computer system which runs the operating workstations; from it, the plant can be brought to a safe shutdown state and accident conditions controlled. This diversified equipment, called "auxiliary panel", is used only when the computer system is unavailable (failure or programmed shutdown). The qualified wall-mounted mimic panel completes the facility.

The breakdown of tasks between the operator and the I & C system (more commonly known as "degrees of automation") is as follows:

- safety-related protective actions are automated; from a safety viewpoint, operator intervention in the 20 minutes following initiation of a protective action is not required,

- actions related to equipment protection are automatic, especially for high-cost items,

- the adjustment functions required to keep the plant stable or to vary plant load are automated,

- there is no sequential automation for function start-up or shutdown; the operator intervenes on a group of actuators executing a limited task, or he controls individual actuators.

4. COMPOSITION AND ORGANISATION OF THE OPERATING TEAM

The operating team is the same as in all EDF nuclear power plants.

For a pair of units, it comprises:

- one shift operations manager, who leads the team. In accident conditions, he acts as safety engineer until the latter arrives.

- two technical supervisors (one per unit), who support the shift operations manager. They play a supervisory role in accident conditions.

- four operators (two per unit; one is responsible for operating the reactor, the other for the water-steam line, particularly in accident conditions).

- two operating technicians to operate the auxiliary nuclear building.

- field operatives (operating technicians and inspection patrols).

5. OPERATING EQUIPMENT AT THE OPERATORS' DISPOSAL

Each of the four operating workstations in the control room includes an operating zone and an alarm zone. When all four are available, two are allocated to unit operation, and two are used for surveillance only (the controls cannot be accessed). If one or two workstations assigned to operation become unavailable, one or both of the other two workstations may be reconfigured into operating mode.

The operating zone consists of three graphic screens, three touch-sensitive screens, a trackball and a function keypad. From it, the operator has access to:

- mimic-type images (about 800) representing either circuits or information and control groups corresponding to an operating task,

- data sheets (about 10,000) providing precise details about each sensor or actuator,

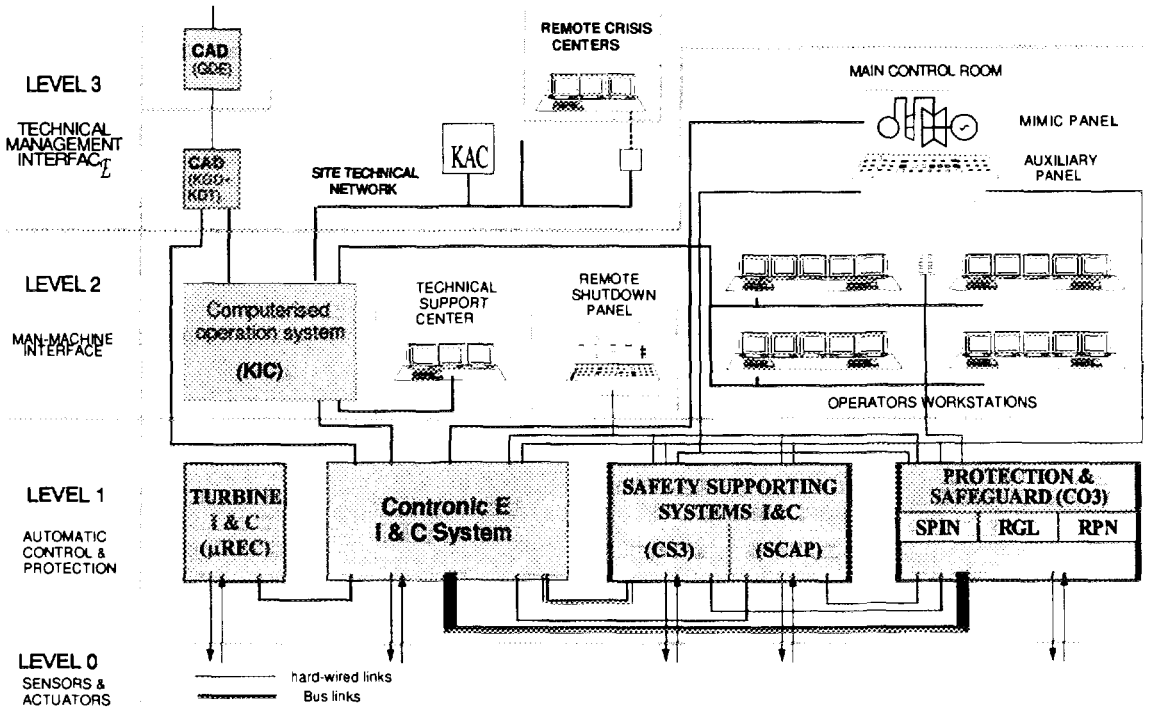
- pages of procedures guiding him through normal operating tasks and during incident and accident operation (about 1,000 and 2,500 respectively). The accident procedures are based on a state-oriented approach.

The alarm zone consists of four semi-graphic screens and a function keypad; it displays alarm messages, which are classified according to severity and degree of urgency.

The operator can process these alarms by calling up, on the operating-zone screen, the alarm sheets (there are about 4,000) which indicate the steps to take and provide the means to do so.

The two operating workstations are standardised, and any unit control or information can be accessed from either workstation. For operation with the procedures, the latter are structured so activities can be shared between the "reactor" operator, the "water-steam" operator and the supervisor.

6. MAIN FEATURES OF THE I&C ARCHITECTURE



I&C architecture of the N4 series

The architecture of the I & C system is structured in:

- a level 1, or "automation" level, comprising:

  - the protection system and the safeguard systems support system, safety classified 1E; these are programmed systems developed specifically for these applications, in accordance with the recommendations of the IEC 880 standard, and which automatically execute all necessary safety-related actions within 20 minutes after an accident.

  - the system that adjusts and protects the turbogenerator; this is a programmed system, supplied with the turbogenerator.

- programmable logic controllers (about 320 PLCs are located in 150 cabinets) in charge of all automatic protection and adjustment; they transmit all acquired information on the process to level 2 and receive the operators' orders from level 2.

- a level 2, or "man-machine interface" level, consisting of:

  - the computer system (KIC) which manages the operator workstations, whose redundant architecture permits a high availability target.

  - the auxiliary panel and mimic panel, whose information and controls are directly linked to level 1.

- a level 3, or "technical management level", comprising :

  - the maintenance or technical aids systems,

  - the links to the National Crisis Centre.

The controls and information on the auxiliary panel are those directly necessary:

- in a normal operating situation, to keep the plant stable or bring it to a safe shutdown state.

- in an accident situation, to apply the accident procedures of the state-oriented approach.

The operating scenarios are as follows:

- KIC fully operational,

  - normal operation: the whole team is in KIC mode.

  - accident operation: the operators and supervisor are working on the KIC and the safety engineer is on the auxiliary panel (this provision was chosen).

- Total KIC failure: the whole team is on the auxiliary panel (in normal conditions, the unit is kept as is for a maximum of four hours).

- Partial KIC failure:

  - normal conditions: the loss of more than three operator workstations results in switchover to the auxiliary panel.

  - accident conditions: the loss of more than two operator workstations results in switchover to the auxiliary panel.

7. DATA MANAGEMENT AND VALIDATION

The term "I & C data" covers various entities:

- "process" data, characterising the sensors and actuators connected to the I & C.
- the processing algorithms (automation - adjustments) located,
    - in the 1E systems.
    - in the PLC's.
- the data generated by the I & C system.
- the images, procedures, alarm sheets.

The data specific to the 1E systems are managed and validated separately.

The other data, which represents about 16 million basic information items (40,000 objects comprising 40 attributes on average), are managed by a CAD tool to ensure their coherence.

The algorithms of the level-1 PLC's were tested on test benches in a design office. The level-2 images and procedures were validated functionally on simulators and, for the syntax, on test benches.

Stringent modification procedures are in place for modifications which prove necessary while the unit is loaded.

Level-1 and level-2 data (excluding the 1E systems) can be modified with systems running and the unit in operation. Only the items (sensors, actuators, images, etc.) whose data are involved in the modifications are considered unavailable by the operators throughout execution of the modification (a few minutes at most).

8. PROVISIONS FOR SYSTEM MAINTENANCE

The system is equipped, in its constituent parts, of self-testing mechanisms which identify failures and trigger the activation of suitable redundancies and diagnosis-assistance mechanisms.

The redundancy levels in place for safety- or availability-related functions, and the functions required for operation, are designed in such a way that the maintenance operations are performed in-line, and the systems remain operational.

To modify the System software, the system in question must be shut down. This type of modification will be carried out during reloading outages.

9. OBJECTIVES ACHIEVED

Today, Chooz NPP unit 1 and 2 are connected to the French grid (since 1996) and the unit of Civaux 1 is in the final phase of commissioning tests. Start up of the last (Civaux 2) is scheduled in summer 1998.

The commissioning hitches inherent to any innovation have been resolved, the safety authority has granted operating licenses.

So far the users are satisfied with the system, and the steps to ensure long service life (procurement of spare-part stocks, long-term contracts with main suppliers) have been taken.

During start-up of the lead unit, the I & C system did not give rise to any noticeable incidents, and malfunctions that occurred during testing were quickly controlled.

The short but significant operating time associated to the commissioning phases have generated a first positive experience feedback which has consolidated the decision made by EDF in the design of this project, as well on the MMI point of view as on the I&C architecture one.

Finally these positive aspects have led to the decision taken by EDF, its European partners in the EURs (European Utilities Requirements) and the German utilities partnering the EPR project (European Pressurised Reactor), to choose this control-room concept for future plants.

10. THE CONDITIONS FOR SUCCESS

Of the many factors that shape the success of such a system, three should be emphasised :

- the project organisation; this was the decisive factor, enabling all the energies of several engineering departments and the suppliers to be properly focused.

- the complementary relationship between designer and utility.

- the quality of the data.

The utility was associated with the study and assessment of the system from the design stage : the utility designed a large proportion of the images, procedures and alarm sheets, while the engineering departments invested great effort in the operating studies and in harmonising the information-processing modes.

The computerised procedures, the design of task-tailored images, and the computerised alarm sheets required heavy design input, as any error or incomplete aspect is more problematic to correct than in the case of paper documentation.

The quality of the information supplied to the operator (accuracy, relevance, etc.) is an essential factor for success: it is fundamentally important for the operator to trust this information. The chosen option - always to leave him in control of the situation (ultimately he decides, not the computer) - also contributes strongly to this trust.