AAEC-LIB/Trans-761

AUSTRALIAN ATOMIC ENERGY COMMISSION RESEARCH ESTABLISHMENT

TAKING HUMAN ERROR INTO ACCOUNT IN THE DESIGN OF NUCLEAR REACTOR CENTRES

by

PROUILLAC, LERAT, JANOIR

(Revue generale nucleaire; no. 5, Sept.-Oct., 1981, pp. 434-440)

Translated from the French by Scientific Information Services, Melbourne

May 1982

AUSTRALIAN ATOMIC ENERGY COMMISSION

LIB/TRANS SERIES

Translations in this series were prepared as working documents for the use of research scientists at the Australian Atomic Energy Commission.

In order that they might be made available with the least possible delay, no attempt has been made to edit them, nor have all typing errors necessarily been identified and corrected.

Copies of translations in this series are made available to interested organizations and individuals only on the express understanding that they may be imperfect and do not aim to meet the standards of a published document. The Commission will not be held responsible for any inaccuracies in the translated text or for any errors resulting therefrom.

If any further reproduction of this translation is made by the recipient thereof, this note must be reproduced together with the text of the translation.

TAKING HUMAN ERROR INTO ACCOUNT IN THE DESIGN OF NUCLEAR REACTOR CENTRES

PROUILLAC AND LERAT (Framatome) and JANDIR (EDF)

The authors study the role of the operator in the centralized management of PRESSURIZED WATER NUCLEAR REACTORS and present the different types of human error likely to arise , and also the means of their prevention or how to mitigate their consequences. In this domain, they describe some of the possible improvements and the putting into operation of them based upon the lessons drawn from experience.

I. INTRODUCTION

A nuclear reactor plant for electricity is a complex installation. Man necessarily plays a role in its management and in the interventions necessary in the plant at shut-down (maintenance and renewal of the combustible elements). The taking into account of the human factor is thus indispensible at the design stage. The designer of the electricity generating nuclear plant is preoccupied the whole of the time with this aspect, but its proper evaluation is not an easy task; the evaluation of the human factor is not an exact science and is only dealt with under difficulty by the engineer who does not have quantitative data on the subject at his disposal.

The advent of nuclear reactor centres, which must not/any more than a very slight residual risk, has given rise to markedly acute problems: the recurrence of experiences in France, as also the notorious accident at Three Mile Island, will call to mind the importance of the human factor.

II. Generalities concerning the role of the operator and of automation.

We are voluntarily restricting our treatment of this vast subject to the role of the operator in the centralized management of pressurized water reactors , a role which is most important at the design stage. We are also leaving to one side, without forgetting the necessity of its correct treatment, the interventions necessary outside the control room during the running or the stoppage of the installation.

The operator entrusted with the centralized management, plays two principal roles. He must carry out the actions of management th- are not entrusted to automation; he must supervise the whole of his installation.

* Primary role ; the management.

The actions carried out by the operator or by automation may be grouped into three classes for an electricity-nuclear reactor :

- the regulation, during functional operation, of certain physical parameters, to adjust them between certain defined limits, by actions taken with other physical parameters,
- the changing of the state of the system (the actions of putting into, or taking out of, service, starting-up operations, shutdown),
- actions to deal with anomalies (protective action against incidents, safe-guarding actions in the case of accident).

Being given the possibility of intervention by a sole operator, the management of a nuclear reactor plant appeals largely for automation. This latter possesses the following advantages:

- its time of reaction is extremely short compared with that of a human operator and is thus very suitable for rapid intervention,
- it reduces the manoeuvres of the operator and thus facilitates his task, it reduces the number of control instruments and simplifies the set-up of the control console display.

It does, however, have disadvantages :

- it has a memory, but is incapable of interpreting a situation that has not been envisaged in advance. It cannot thus be used unless the laws connecting the parameters are well understood, and unless the possible situations which have to be faced up to have been completely identified,
- likewise, for changing the state of the system , it lacks flexibility and leads to restriction in advance to a reduced number of situations , which could occasion difficulties for the user,
- finally, it is not free from defects either.

In conclusion, a compromise should be found between actions which are automated and those taken by humans, as a function of the nature and of the knowledge of the situation which must be faced up to.

* Second role : surveillance.

The operator must continually supervise the installation in its entirety in order to carry out the actions within his jurisdiction, or make up for any defects in the automation system.

He should be able to :
- verify the correct functioning of the automation devices,
- be alert to the presence of a defect and be able to identify it,
- diagnose the situation from the consistency or not of significant parameters and by reference to management procedures.

Salle de commande de la centrale de Bugey. Control room at Bugey

III. Generalities concerning human errors. Remedies.

The analysis of the human factor has given and is giving, rise to numerous studies.

We have classified the human errors schematically into four types (this concerns, in fact, the actions which are unsuited to the situation in the installation) :

- First type :

The actions of management and the associated surveillance to be carried out are in excess of the capability of the normal human being who can thus not cope with them properly : they are too delicate or involved, or too numerous to handle in the time available, or happening too fast to handle.

- Second type :

The operator has been well instructed and knows what is to be done, but he does not act correctly because of hastiness, or because of distraction, or simply by neglect. The error is therefore a limited and temporary one.

- Third type :

The operator is mislead in his action by inadequate or erroneous information: absence of pertinent information, errors of (instrument) reading, overwhelming amount of information in an avalanche.

- Fourth type :

The operator sees that his means are limited for various reasons : physiological, psychological or by insufficiency of information. In spite of the information he is given he makes a diagnostic error. Such types of error happen quite commonly and because of this may take a dramatic turn. The accident at Three Mile Island illustrates this abundantly. This type of error is frequently associated with the preceding one.

What should be done by the designer to avoid or mitigate these various types of error ?

The first type could be avoided by adequate automation.

The second type as far as they concern errors of manipulation which are the most damaging with regard to the possibility of their reduction and with regard to safety of the installation, should be preventable by the provision of interlocking controls. As far as forgetting or omissions with serious consequences are concerned, this could be avoided by automation.

The third type could be reduced by the design and presentation which is more appropriate of the information. But the problem of the processing of the information remains a difficult one, even though the actual information devices present us with vast range of possibilities.

The fourth type, and the most serious, could be avoided by reducing the possibilities of intervention on the part of the operator and thus by further increasing the automation with the limits indicated and which give him (the operator) adequately diversified information.

For all the types of error the ergonomic design of the work station exercises a significant influence. It encompasses a number of factors : noise, temperature, lighting and colors, height and extent of the working area, regard for stereotyped actions, etc.

In resume, the designer should take human fallibility into account in the design of the control room and of the control-regulating instruments, in particular with regard to the level of automation and the choice of control instruments, for the information placed at the disposal of the operator, and for the laying-out of the control room.

IV. ORIGINAL DESIGN (900 MW).

IV.1 Level of automation.

The necessity and the opportunity of automation of an action or a sequence of actions depends upon the following criteria :
a) frequency of intervention necessitated by this action,
b) number of manoeuvres to be carried out in a given time,
c) delay time available to carry out the action or sequence of actions, starting from the detection of an abnormal situation, with the objective of preventing serious consequences,
d) the seriousness of an omission in the execution of an action.

These different criteria are applicable, as follows, in different functional situations.

IV.1.1. Adjustment of physical parameters.

Analog adjustments which require continuous intervention, are completely automated in normal service.

IV.1.2. Action in case of an incident or an accident.

When the defect develops rapidly or when an omission on the part of the operator is serious for overcoming the difficulty or because of the damage occasioned, the protection is generally automatic.

This is always the case when the intervention is to ward off an incident which places the safety of the nuclear plant at risk, or for reducing the consequences of a nuclear accident where the intervention is indispensible within a lapse of time of 10 minutes. Also the shut-down in case of urgency, the isolation of the containment, and the injection of the control rods for security are automated.

In the contrary case, the operator himself should be able to initiate the protective measures.

In resume, the level of automation of the systems of nuclear protection and safeguards is very high; except for certain specific actions (tripping of the primary pump in the case of rupture of the primary line (= cold leg ?), the time lapse for intervention by the operator is in fact in the neighbourhood of thirty minutes. However, beyond this period of time, in an accident situation, the operator is constrained to act on his own initiative in order to restore the installation to a state of safe withdrawal; it is thus unthinkable, given the multitude of situations which may be envisaged and the (im)possibility of being able to identify them all in advance, to entrust the sequence of operations required to automation.

IV.1.3. Changing the state of the system.

For this the level of automation is determined by the number of manoeuvres necessary for the passage from one state to another.

For the heater (boiler) , due to the fact that certain circuits are allocated to certain different functions this necessitates different configurations, the level retained is the individual control for each of the activating mechanisms (switches). For the machine room , the level retained is the functional control of the principal actuator (simultaneous control of the principal switch and of its satellite switches).

However, the operator frequently has at his disposal for the heater a grouping of certain actions relative to the same safety function (isolation of containment - security injection (of control rods)). Furthermore, certain controls, such as the insertion of the grapples for control of the reactor with overlapping (over-riding) of the groups, borification (with borax-water solution) , are likewise grouped together.

In resume, in the French nuclear reactors, the changing of state is only automated to a slight extent which allows for a gain in flexibility of the functioning.

IV. INTERVENTION DEVICES - INTERLOCKING.

For carrying out the management actions, the operator has means at his disposal in the control room which allow him :
- to control the manoeuvring of the actuators - switches - (turning-boosting of lights),
- to effect the adjustments or to supplement the automatic analog adjustments (hand control relays, intermediate or semi-manual relays),
- to make a choice (commutators automatic-manual, commutators - switches - for the choice of redundant auxiliaries).

The layouts are arranged to avoid manipulative errors of the more serious sort (type 2).

Provision is also made in the design of the interlocking controls for co-ordinating the actions of the operator with the automation devices; for example, it is impossible to to halt a protective action before it has been completely executed.

In a similar fashion, use is made of covers for the control buttons and the interlocking devices associated with them which are opened and shut with keys. These latter are provided at the time of putting into, or taking out of, service of the equipment, in order to remind the operator that certain conditions should be fulfilled as a preliminary operation. This is the case, for example, when putting the primary pump into service and also the charging pump.

IV.3. INFORMATION FOR THE OPERATOR.

The information is given by classical means and by complementary information processing (TCI) which utilizes an industrial computer.

IV.3.1. The classical means are :

- for information relating to state :

* pilot-lights associated with TPL,
* pilot-lights of state (position of valves for isolation of containment)
* illuminated glass-globes,

- for analog information :
* recorders and indicators

- for information of defects :
* illuminated alarm glass-globes (warning-signal lights).

The illuminated warning signals are arranged in four categories corresponding to a hierarchy of the degree of urgency of the reaction of the operator for re-establishing proper control of the situation :

- category 1 on red background calls for immediate action,
- category 2 on a yellow background calls for a different action (than that performed ?),
- category 3 on a white background indicates a change of state not caused by operator action,
- category 4 on a green background indicates a fault treated automatically with passage to null charge..

IV.3.2. The information for normal management and for incidents are likewise processed by the TCI, which transmits the information to the display devices adapted to the various user requirements (VDU's, printers, magnetic tapes).

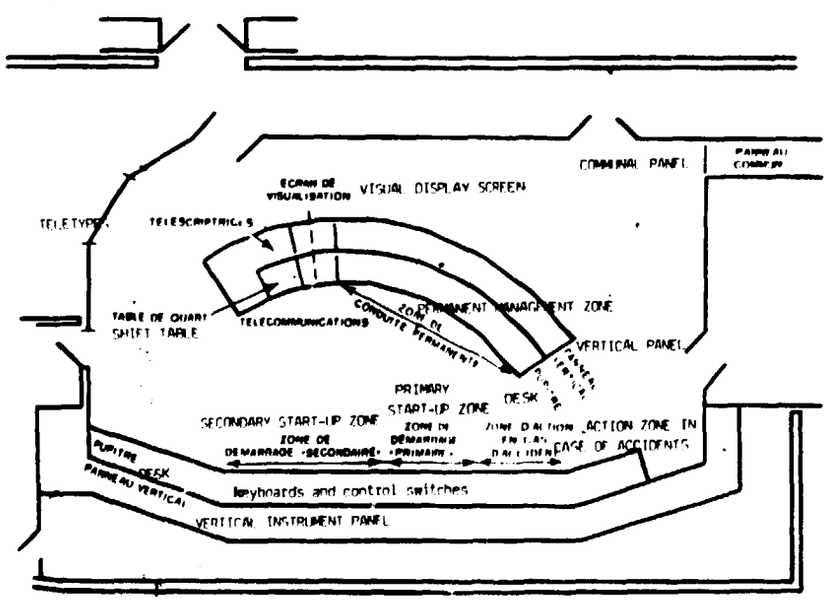


Schéma de la salle de commande du Bugey, prototype de la salle de commande de CP1

Diagram of control room at Bugey, prototype of the CP1 control room

The visual display screens are three in number :
- a management screen giving direct information (discrepancies, alarms),
- a screen for interactive dialogues permitting more complete information,
- a progress display screen (following-up consistency of parameter, map of the core).

There are three printers.

The information is likewise handled by an a posteriori analysis function on various items of equipment: oscilloperturbography, TCI ; this analysis function carries out the preparation of a daily work log and an "historical" record of events.

IV.4. DESIGN OF THE CONTROL ROOM (900 MW).

The control room of CPI consists of a central desk with keyboards, etc., arranged on the arc of a circle and a vertical instrument read-out panel behind it. The control devices and regulatory equipment are grouped in zones of management and are four in number :

- normal management zone on the central desk,
- safety systems management zone,
- start-up zone for the heater (boiler),
- start-up zone for the machine room.

The CPI control room gives precedence to normal management.

The controls for less frequent manoeuvres (distribution of electricity, test procedures, chemical measurements) are located at the ends of the rear display panel.

An external corridor connects the locations situated on either side of the control room, ensuring that the room is not used as a passage-way. An efficient air-conditioning system maintains the correct temperature and humidity. The indirect lighting is adjusted in intensity and distribution for the avoidance of reflections. The colors of the different elements are appropriately chosen. The room is also as free from noise as possible, being well insulated.

V. LESSONS FROM EXPERIENCE.

V.1. Lessons learned in France on the reactor and on the simulator.

These have been obtained at three levels :

V.1.1. Difficulties at certain phases of management.

Certain phases of management are complex for the operators; an important case is encountered during the start-up of the reactor in the monophasic situation; therefore improvements have been made to the system and the regulation of the primary pressure has been adapted to this situation; specific alarms have been installed.

V.1.2. Opportunity to improve information processing.

When shutting-down the reactor some alarms may be given which do not correspond to real defects in this situation. Modifications, envisaged to remedy this situation, have been studied and now have already been introduced for the reactors at Bugey. These are in the course of being introduced at CPI also.

Futhermore, in an incident or accident situation, the operator finds himself in the presence of an avalanche of alarms (for example, after an emergency shutdown (scram) or a security injection) without being able to distinguish the defect or cause of the incident from those which are of no consequence. Under these conditions the diagnostics of the incident are not easily made. Some way of processing the alarms is very desirable.

V.1.3. Opportunity to improve the control room 900.

Experience has made the disadvantages of the CPI architecture stand out very clearly.

It has actually been found :
- on the central desk, the controls necessary at the time of normal service and for start-up and shut-down,
- on the rear display panel,the controls peculiar to start-up and shut-down.

Thus in a period of start-up/shut-down the operater is condemned to making frequent visits between the central desk and the display panel.

The same may be asserted about the information devices which are sometimes spread out over the desk and the display screen.

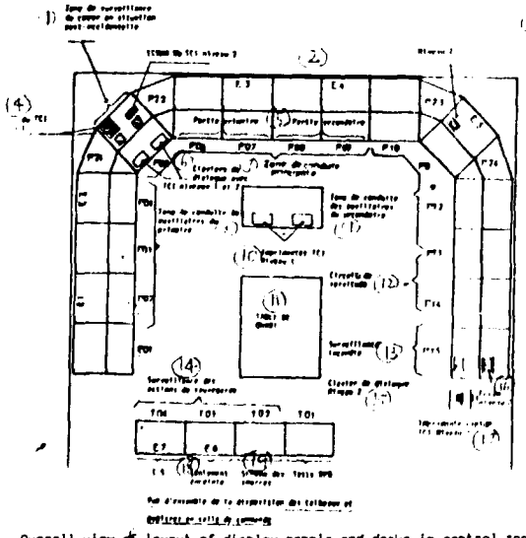
A unique (single) desk console and instrument panel such as has been conceived for Fessenheim, by way of an exceptional example, provides a common frontier between the two zones under consideration and thus permits of a readily attainable regrouping of all of the functions. It also gives better scope for the implementation of the synoptics and for the development of the visual display screens' role.

V.2. LESSONS FROM THREE MILE ISLAND.

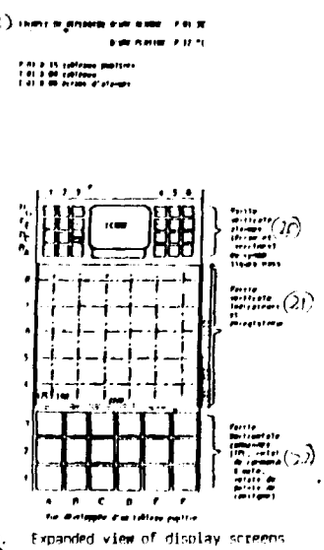
The accident at TMI has revealed that the aptitude of the operator to react correctly in an accident situation could actually fall short of the general expectations of the designer. The latter has then become aware that it is necessary to assist the operator to a greater extent in these difficult circumstances and that the means placed at his disposal up to that time could prove insufficient in a deteriorated situation. More precisely, the lessons have been learned regarding the three following points :

Annotations to Diagram below (reference numbers shown in red)

1. Surveillance zone for core in post-accident situation
2. VDU screens for TCI, level 2
3. EXAMPLE OF LOCATION OF AN ALARM : P 01 3C
   OF A PLATEN : P 12 D1
   P 01 à 15 display panels desks
   T 01 à 04 display panels
   E 01 à 06 alarm screen
4. VDU screens for TCI , level 1
5. Primary part Secondary part
6. Keyboards for dialoque with TCI , levels 1 and 2
7. Principal management zone
8. Management zone for primary auxiliaries
9. Management zone for secondary auxiliaries
10. Printers for TCI, level 1
11. Shift-team table
12. "servitude" (slave) circuits
13. Fire surveillance
14. Safeguard actions surveillance
15. Dialoque keyboard, level 2
16. Display screen, level 2
17. High-speed printer, TCI, level 2
18. Isolation of containment
19. Source diagram
20. Vertical portion of alarms (screen and illuminated glass warning lights) or synoptics
21. Vertical portion:
    indicators and re orders
22. Horizontal portion of controls (TPL, relays for manual control, relais for points of orders).



Overall view of layout of display panels and desks in control room.
Schéma de la salle de commande 1300



Expanded view of display screens and controls desk

Layout of control room for 1300 MW PWR

V.2.1. Improvement of the instrumentation.

Two causes for concern emerge :

a) The validity of the information. The order of closure of a valve must not be confounded with the information of the position of closure of a valve - which has been avoided in France - and the information is to be taken from the stem of the valve and not from that of the servo-motor. Furthermore, the domain of validity of certain measurements should be enlarged (example : measurement of the core temperature).

b) The investigation of supplementary measurements which allow for being informed of the state of safety of the core, and of things included in the degradation state : level of water in the vessel of reactor and the presence of non-condensible substances.

V.2.2. Improvement of information processing in an accident situation.

There also, it is apparent that there was a surplus of alarms, so that it would be advisable to inhibit those that are not significant in such a situation and to arrange the others in a hierarchy.
Certain of the processing should be done with the objective of facilitating the diagnosis by the operator (for example, calculation of the reserve factor for boiling in the reactor vessel). A particular effort should likewise be made in the presentation of information, by grouping together the information useful in such a situation, and making clearly apparent the safety of the reactor core.

V.2.3. Addition of some automation judged to be necessary

so that the tele-control of the iodine filters allows for purification before rejection. It should be emphasized that only a few of the improvements have appeared to be possible in this domain.

A very important program has been undertaken in France following the TMI accident. Certain improvements have already been implemented on the 900, other aspects are under further study.

VI. EVOLUTION OF THE DESIGN. APPLICATION TO THE 1300 (MW reactor).

VI.1. Management - Automation.

In the assembly, the same principles as for the 900 are applicable. However it has been essential to facilitate the management of the reactor and thus to reduce the number of control instruments and to enhance the level of automation of the changing of state.

With respect to the heater, this effort has proved to be somewhat in vain and in this there has remained only a few of the things relevant to the design of the 900. We draw attention however to certain limited modifications : addition of specific automation for the closure of the spray valves of the pressuriser, introduction of interlocking at a supplementary level (putting the RRA pump into operation).

In the machine room, on the other hand, a grouping of the controls for the elementary functions is operative when functional studies do not make them appear to be disadvantageous.

It was thus not actually envisaged to bring about the evolution, in a very noticeable fashion, of the level of automation of the 1300 MW reactor in relation to that of the 900.

VI.2. Information - surveillance.

This is the domain in which the evolution is the most important.

This is related to :
- the instrumentation utilized,
- the treatments effected (or processing of information),
- method of presentation of information.

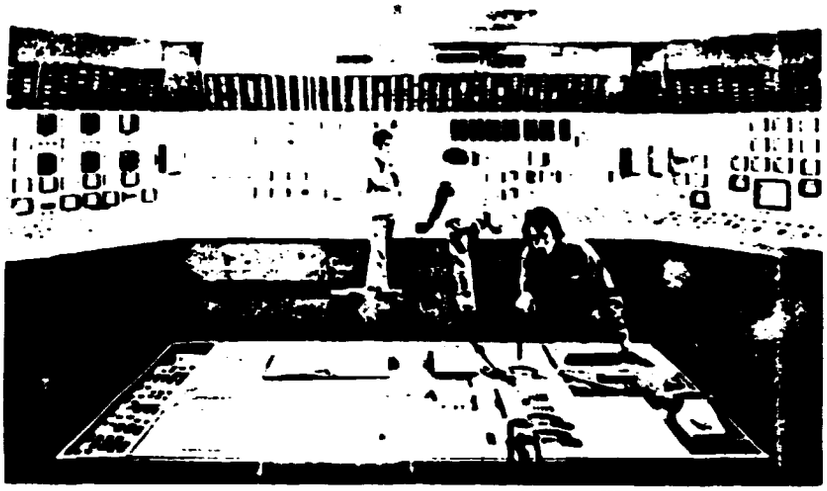
VI.2.1. Instrumentation.

A post-accident system of surveillance has been studied (application of Regulator Guide 1-97).
Besides this an effort is being made with a view of carrying on the development or of improving the performance with new measurements (level of the vessel, degree of vacuum) for degraded states. The application to the various "PALIERS" (= bearings or supports ??) has not been defined for the time being.

Particular attention has been paid to the validity of the measurements (corrections, surveillance, qualification for the ambient conditions). In this regard, the comparison of values issued by the redundant receptors will be, on the 1300, carried out by the TCI (complementary data processor).

VI.2.2. Information processing.

The lessons learned from experience have led to placing the information at the disposal of the operator in the form of tree-diagrams and hierarchies. For this purpose an effort has been made in three directions;
- improvement of considerable extent in the processing of the alarms with a view to not furnishing the operator with other alarms than those representative of an actual defect in the installation and not to provide him with alarms other than those provoked by the appearance of this defect and not those due to the security actions initiated by this defect; also, as a general rule, the alarms signalling the exceeding of physical criteria which it is normal to have are inhibited, taking into account the state of the reactor core; furthermore, during an emergency shut-down (scram) and the initiation of protective action, the operator will not be furnished with an alarm other than the initiation of the security action and the alarms subsequent to this initiation will be inhibited,
- processing of aids for the operator in normal situations : this concerns essentially , of the steering aids with the view to optimizing the intervention of the operator,
- processing of operational aids in an accident situation.



Salle de commande de Fessenheim, prototype de la salle 1300.

Control room at Fessenheim, prototype for 1300

These processing operations consist of :

* grouping of the essential information for the surveillance of the progress of the safe-guard actions,

* an attempt to identify, by correlation, the situation of the reactor core vis-a-vis the vital parameters, such as the balance of primary water (this is concerned with a limited application of the approach by states defined in VI.3),

* guiding the operator in his diagnosis and assisting him, by automatic processing of information, to choose the correct procedure.

A study of these modifications is underway on the 1300 MW PWR.

VI.2.3. Presentation of the information.

The details of information presentation on the 1300 are notably :
- the alarms of category 1 shown on the glass panel warning-signal lights,
- the alarms of categories 2, 3 and 4 are displayed on the 2 VDU screens,
- 5 color VDU screens are envisaged for the TCI (complementary information processor)

This development in the use of display screens, allowing for enhanced flexibility in the presentation display of information, should be further developed on the N4 (see further on).

VI.3. Approach by states.

The management procedures in an actual post-accident situation are drafted on the basis of the study of standard sequences.

The initial procedure of diagnostic aid consists of identifying, in accordance with the development of significant parameters, the type of accident in such a way as to be able to use the corresponding post-accident procedure. This approach is rendered difficult because it is not possible to envisage in an exhaustive manner all of the possible scenarios of accident in which is included more especially the probable or possible errors made by the operator and also the equipment failures.

Another type of approach (called the approach by states) is at present actually under study, has thus been envisaged with the objective of furnishing the operator with details of the operations to be carried out as a unique function of the state of the installation, independent of the type of accident, of the defects of the equipment or the possible errors made by the operator in the initial phase. It thus offers to the operator the very interesting possibility of making good the situation, when he did not know, as at Three Mile Island, how to identify the accident sequence.

This approach consists of making an exhaustive inventory of the thermodynamic state of the heater starting out from the mode of circulation of the liquid (forced or natural circulation), of the state of the liquid (monophasic or diphasic) and the mass balance, the energy balance and the amount of movement.

These states, characterized by a reduced number of physical parameters (primary pressure, primary temperature, margin of sub-saturation or monophasic.....being known, it is thus possible to specify for the operator the actions necessary to be taken to stabilize the heater in a cooling mode (for example, in augmenting or diminishing the inventory of mass) or to restore it to another mode that is adjudged safer.

In the case where the means to be adopted are not available at the moment, the installation will develop towards another state for which the actions to be performed, called the ultimate, will be the same as specified.

This approach, complementary to that actually in use, necessitates, however, the employment of supplementary information (inventory of the water coolant in the reactor vessel, degree of vacuum in the hot water reticulation pipes,.....) in order to characterize, without ambiguity, the different states in a situation which has deteriorated gravely.

There is, at the present time, a great hope of being able to get a better control over this promising approach vis-a-vis the problems of human fallibility in the accident situation.

VI.4. General design of the control room.

An effort has been made to modernize the control room, to improve the presentation of information by means of a better arrangement of the control and regulators instruments, by a much greater recourse to equipment developed by "Hardware" and a grouping of the necessary instruments, in particular in an accident situation.

The control room of the 1300 comprises, like that at Fessenheim, a large console desk and instrument display panel and a rear instrument display panel grouping together all the instruments for the management operations and for the display of the associated information.

For a satisfactory grouping of instruments related to the same function, the equipment is grouped in different zones of management from that at CPI. The principal management zone close to the zone of surveillance of the core in an accident situation collects together all the necessary instrumentation :
- for regulation of the charge (regulation of the turbine, alternator),
- for regulation of the neutron population strength,
- for regulation of the primary pressure,
- for supplying the steam generator (normal and relief),
- for regulation of the output of the turbine by-pass,
- for emergency shut-down and disconnection of the turbine.

VII. Future development. "Palier N°". (Translator's note: "Palier" generally means a bearing or support of some kind, but no specific meaning can be found for this particular usage which may refer to the whole of the installation with the containment; the term 'palier' will thus be used in what follows in the absence of more specific information in relation to PWRs).

The actual delays in the construct of the 1300 have not allowed for the gaining all the benefits of the fruit of the lessons learned from experience. Also for the future palier, called "Palier N4", a global review is being undertaken with a view to adapting the controls-regulators and the control room to the newer concepts of utilization in different normal situations, accident situations and post-accident situations.

The point of departure for this review is a functional analysis based not only on the data of elementary systems as at other times, but also on the management procedures, alarm documentation and the aptitude of the operator such as that derived from experience of operation acquired not only in the nuclear centre itself but also on the simulator.

The purpose of this analysis is to identify the different assistance activities for the management, the correlation of the data to be developed and the different elements to be taken into account in the design of the control room.

A simulator should be available for use, which allows for programming and implementation of the treatments and correlations previously mentioned and for the validation of the conception and design of the whole of the control room. Finally, a technological study, with a view to adapting the existing equipment to definite requirements, to simplification of the interfaces, to standardization of the exchange of information, has likewise been launched.

This review largely calls upon the resources of the EDF (French Electricity Authority). The construction firm of Framatome is also involved in the project.

This study which was launched in October 1980 should be finished in 1984.

VII. Conclusion.

This review of experience has placed the accent on taking the human factor into account in the design of nuclear centres. Important studies have been undertaken not only with the construction engineers but also with EDF with a view of applying desirable improvements to French nuclear reactors in this domain. These studies are a long way off completion in a concrete sense; this results from their complexity and from the necessity also to carry out analyses in depth before drawing conclusions so as to avoid these latter being unsuited to the purpose, and finally from the difficulties encountered in the administration of these improvements applicable to the numerous nuclear reactors in all stages of advancement possible since the advance project is in the stage of industrial usage.

. . . . . .

Prise en compte de la fiabilité humaine dans la conception des centrales nucléaires

Par MM. PROUILLAC et LERAT,
Framatome,
et JANOIR,
EDF.

Les auteurs étudient le rôle de l'opérateur dans la conduite centralisée des tranches nucléaires à eau pressurisée. Ils présentent les différents types de défaillances humaines pouvant survenir ainsi que les moyens susceptibles de les éviter ou de maîtriser leurs conséquences. Ils décrivent, dans ce domaine, les améliorations possibles ou mises en œuvre se dégageant des enseignements tirés de l'expérience.

I. Introduction.

Une tranche électro-nucléaire est une installation complexe. L'homme joue nécessairement un rôle dans sa conduite et dans les interventions sur cette tranche à l'arrêt (entretien, renouvellement du combustible). La prise en compte du facteur humain à la conception est donc indispensable. Le concepteur de centrales électrogènes s'en est de tout temps préoccupé, mais cette prise en compte n'est pas aisée : l'évaluation du facteur humain ne relève pas d'une science exacte et est difficilement saisissable par l'ingénieur qui manque à son sujet de données quantitatives.

L'avènement des centrales nucléaires, qui ne doivent présenter qu'un risque résiduel très faible, a donné au problème une acuité marquée ; le retour de l'expérience en France, comme le célèbre accident de TMI, devaient rappeler l'importance du facteur humain.

II. Généralités sur les rôles de l'opérateur et de l'automatisme.

Nous circonscrirons volontairement notre vaste sujet au rôle de l'opérateur dans la conduite centralisée des tranches à eau pressurisée, rôle le plus important au stade de la conception. Nous laisserons ainsi de côté, sans méconnaître la nécessité de la traiter correctement, l'intervention hors salle de commande sur l'installation en marche ou à l'arrêt.

L'opérateur, chargé de la conduite centralisée, joue deux rôles principaux. Il doit réaliser les actions de conduite non confiées aux automatismes ; il doit surveiller son installation.

• Premier rôle : la conduite.

Les actions réalisées sur une tranche électro-nucléaire par l'opérateur ou l'automatisme se regroupent en trois classes :

- le réglage pendant le fonctionnement, de certains paramètres physiques entre des limites définies, par action sur d'autres paramètres physiques,
- les changements d'états des systèmes (action de mise en et hors service, action de démarrage, arrêt),
- l'action sur anomalie (action de protection sur incident, action de sauvegarde sur accident).

Il est donné les possibilités d'intervention d'un opérateur seul, la conduite d'une tranche nucléaire fait largement appel à l'automatisme. Celui-ci présente les avantages suivants :

- il a un temps de réaction extrêmement court, comparé à celui de l'homme et donc bien adapté aux interventions rapides,
- il réduit les manœuvres de l'opérateur donc facilite sa tâche ; corrélativement, il réduit le nombre des moyens de commande et simplifie la présentation du tableau de commande.

Il présente, toutefois, des inconvénients :

- il a une mémoire, mais est incapable d'interpréter une situation non prévue à l'avance. Il ne peut donc être utilisé que lorsque les lois entre les paramètres sont bien connues et lorsque les situations possibles, auxquelles il faut faire face, sont toutes identifiées,
- de même pour les changements d'états des systèmes : il manque de souplesse et conduit à figer à l'avance un nombre réduit de situations qui peut constituer une gêne pour l'exploitant,
- enfin, il n'est pas exempt non plus de défaillances.

Finalement, un compromis doit être trouvé entre les actions automatique et humaine, en fonction de la nature et de la connaissance des situations auxquelles il faut faire face.

• Deuxième rôle : surveillance.

L'opérateur doit en permanence surveiller l'ensemble de l'installation pour exécuter les actions de son ressort ou suppléer l'automatisme lorsqu'il est défaillant.

Il doit pouvoir :

- vérifier le fonctionnement correct des automatismes,
- être alerté de la présence d'un défaut et identifier celui-ci,
- faire un diagnostic de la situation par le suivi des paramètres significatifs et par référence aux procédures de conduite.

Salle de commande de la centrale du Bugey.

III. Généralités sur les défaillances humaines. Remèdes.

L'analyse du facteur humain a donné et donne lieu à de nombreux travaux.

Nous classerons schématiquement les défaillance humaines en quatre types (il s'agit, en fait, des actions inadaptées à la situation de l'installation) :

— Premier type.

Les actions de conduite et de surveillance associées, à exécuter, dépassent les possibilités normales de l'homme, qui ne peut donc les assumer correctement : elles sont trop délicates, ou trop nombreuses pour le temps imparti, ou trop rapides à effectuer.

— Deuxième type.

L'opérateur est bien renseigné et sait ce qu'il a à faire, mais il n'agit pas correctement, par précipitation, ou par distraction, ou par omission. La défaillance est alors ponctuel'e.

— Troisième type.

L'opérateur est trahi, dans son action, par une information erronée ou inadéquate : manque d'informations pertinentes, erreur de lecture, avalanche d'informations.

— Quatrième type.

L'opérateur voit ses moyens limités pour des raisons diverses : physiologiques, psychologiques ou par insuffisance de formation. En dépit de l'information qui lui est donnée, il fait une erreur de diagnostic. Une telle défaillance relève du mode commun et de ce fait peut prendre un tour dramatique. L'accident de TMI l'a abondamment illustré. Ce type est souvent associé au précédent.

Que peut faire le concepteur pour éviter ou pallier ces divers types de défaillances ?

Le premier doit être évité par des automatismes adéquats.

Le deuxième type, pour ce qui concerne les erreurs de manipulation les plus néfastes pour la disponibilité et la sûreté, peut être prévenu par les verrouillages. Quant aux oublis et omissions aux conséquences graves, ils doivent être évités par l'automatisme.

Le troisième peut se réduire par une conception et une présentation plus appropriées de l'information. Mais le problème du traitement de l'information reste difficile, même si les moyens informatiques actuels nous offrent de vastes possibilités.

Le quatrième, le plus grave, peut se prévenir en réduisant les possibilités d'intervention de l'opérateur, donc en accroissant encore l'automatisme avec les limites signalées, et en lui donnant une information diversifiée adéquate.

Pour tous les types, la conception ergonomique du poste de travail exerce une influence significative. Elle englobe de nombreux facteurs : bruits, température, éclairages et couleurs, hauteur-éloignement des plans de travail, respect des stéréotypes, etc.

En résumé, le concepteur prendra en compte la fiabilité humaine dans la conception de la salle de commande et du contrôle-commande, en particulier par le niveau d'automatisme et les moyens de commande choisis, par l'information mise à disposition de l'opérateur, par l'aménagement de la salle de commande.

IV. Conception initiale (900 MW).

IV.1. Niveau d'automatisme.

La nécessité, l'opportunité d'automatiser une action ou séquence d'actions dépendent dse critères suivants :
a) fréquence d'intervention nécessitée par cette action,
b) nombre de manœuvres à effectuer dans un temps donné,
c) délai disponible pour effectuer l'action ou séquence à partir de la détection d'une situation anormale, afin d'éviter des conséquences graves,
d) la gravité d'une omission dans l'exécution de l'action.

Ces différents critères s'appliquent, comme suit, dans les différentes situations de fonctionnement.

IV.1.1. Réglage des paramètres physiques.

Les réglages analogiques, qui nécessitent des interventions continues, sont complètement automatisés en service normal.

IV.1.2. Action en cas d'incident ou d'accident.

Lorsque le défaut est à évolution rapide ou lorsqu'une omission de l'opérateur est grave pour la disponibilité ou par les dégâts provoqués, les protections sont généralement automatiques.

Elles le sont toujours lorsque l'intervention parant à un incident risquant d'affecter la sûreté nucléaire ou réduisant les conséquences d'un accident nucléaire est indispensable dans un délai de dix minutes. Ainsi l'arrêt d'urgence, l'isolement d'enceinte, l'injection de sécurité sont automatiques.

Dans le cas contraire, l'opérateur peut mettre en œuvre lui-même la protection.

En résumé, le niveau d'automatisme des systèmes de protection nucléaire et de sauvegarde est élevé ; sauf pour certaines actions spécifiques (déclenchement des pompes primaires en cas de brèche primaire...), le délai d'intervention de l'opérateur est, en fait, voisin de trente minutes. Toutefois, au-delà de ce laps de temps, en situation accidentelle, l'opérateur est contraint d'agir lui-même pour ramener l'installation en état de repli sûr ; il est alors impensable, étant donné la multitude des situations envisageables et la possibilité de les identifier toutes à l'avance, de confier la suite des opérations à l'automatisme.

IV.1.3. Changement d'états des systèmes.

Pour ceux-ci, le niveau d'automatisme traduit le nombre de manœuvres nécessaires au passage d'un état à un autre.

Pour la chaudière, du fait que certains circuits assurent des fonctions différentes nécessitant des configurations différentes, le niveau retenu est la commande individuelle par actionneur. Pour la salle des machines, le niveau retenu est la commande fonctionnelle d'actionneur principal (commande simultanée d'un actionneur principal et de ses actionneurs satellites).

Toutefois, l'opérateur dispose sur la chaudière fréquemment d'un regroupement de certaines actions relatives à une même fonction de sûreté (isolement enceinte-injection de sécurité). En outre, certaines commandes, telles que l'insertion des grappes de commande du réacteur avec chevauchement des groupes, la borification, sont également regroupées.

En résumé, sur les tranches nucléaires françaises, les changements d'états des systèmes sont peu automatisés, ce qui permet de gagner en souplesse de fonctionnement.

IV.2. Moyens d'intervention - Verrouillages.

Pour exécuter ses actions de conduite, l'opérateur dispose en salle de commande de moyens lui permettant :

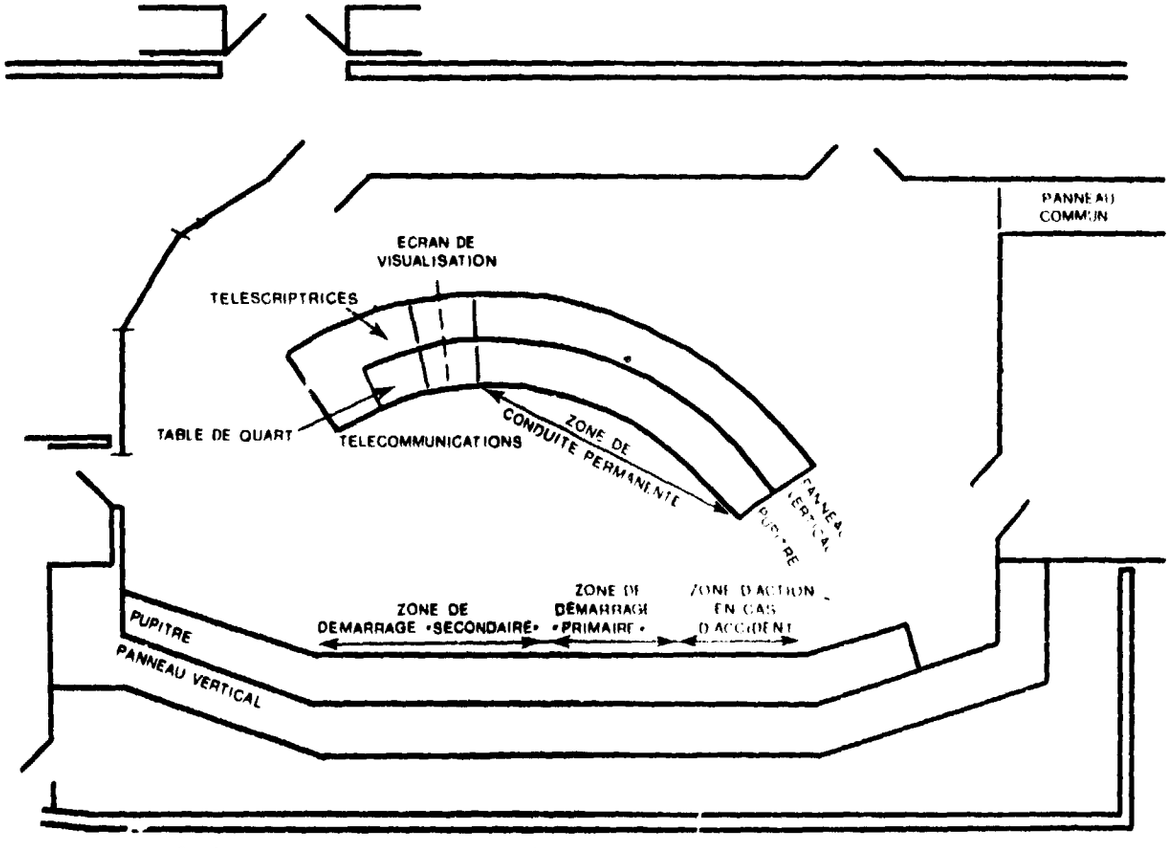


Schéma de la salle de commande du Bugey, prototype de la salle de commande de CP1.

— de commander la manœuvre d'actionneurs (tourner-pousser lumineux),
— d'effectuer des ajustements ou de suppléer les réglages analogiques automatiques (relais de commande à main, relais de commande intermédiaire),
— d'effectuer des choix (commutateurs automatiques-manuels, commutateurs de choix d'auxiliaires redondants).

Des dispositions sont prises pour éviter les erreurs de manipulation les plus graves (type 2).

Ainsi sont prévus à la conception des verrouillages de l'action de l'opérateur par les automatismes ; par exemple, il est impossible d'arrêter une action de protection avant qu'elle ne soit totalement exécutée.

On utilise également le capotage des boutons de commandes et les verrouillages de ceux-ci par clef. Ces derniers sont prévus à la mise en ou hors service d'équipement, pour rappeler à l'opérateur que certaines conditions doivent être préalablement respectées. C'est le cas, par exemple, pour la mise en service des pompes primaires ou des pompes de charge.

IV.3. Informations de l'opérateur.

Les informations sont données par des moyens classiques et par le traitement complémentaire d'informations (TCI) qui utilise un calculateur industriel.

IV.3.1. Les moyens classiques sont

— pour les informations d'état :
  • les voyants associés aux TOR,
  • les voyants d'état (position vannes d'isolement enceinte),
  • les verrines lumineuses,
— pour les informations analogiques :
  • les enregistreurs et indicateurs,
— pour les informations de défaut :
  • les verrines d'alarmes lumineuses.

Les verrines d'alarmes lumineuses se rangent en quatre catégories correspondant à une hiérarchisation du degré d'urgence de la réaction de l'opérateur pour rétablir la situation :
— la catégorie 1 sur fond rouge réclame une action immédiate,
— la catégorie 2 sur fond jaune réclame une action différée,
— la catégorie 3 sur fond blanc indique un changement d'état sans action de l'opérateur,
— la catégorie 4 sur fond vert indique un défaut traité automatiquement avec passage à charge nulle.

IV.3.2. Les informations en conduite normale et incidentelle sont également fournies par le TCI, qui les délivre sur des supports adaptés aux différents utilisateurs (écrans de visualisation, imprimantes, rubans magnétiques).

Les écrans sont au nombre de trois :
— un écran conduite donnant une information directe (discordance, alarmes),
— un écran dialogue permettant une information plus complète,
— un écran évolution (suivi d'un paramètre, carte cœur).

Les imprimantes sont au nombre de trois.

Des informations sont également fournies pour la fonction d'analyse a posteriori sur des appareils divers : oscilloperturbographe, TCI ; cette fonction réalise l'élaboration d'un « Journal de bord » et d'un « Historique ».

IV.4. Conception de la salle de commande (900 MW).

La salle de commande CP1 comporte un pupitre central en arc de cercle et un tableau pupitre arrière. Les moyens de commande et de contrôle sont regroupés par zones de conduite au nombre de quatre :
— zone de conduite normale sur le pupitre central,
— zone de conduite des systèmes de sûreté,
— zone de démarrage de la chaudière,
— zone de démarrage de la salle des machines.

La salle CP1 privilégie la conduite normale.

Les commandes pour manœuvres peu fréquentes (distribution électrique, tests, mesures chimiques) sont reportées aux extrémités du tableau arrière.

Un couloir extérieur relie les locaux situés de part et d'autre de la salle de commande, évitant que celle-ci soit un lieu de passage. Un conditionnement d'air efficace y maintient la température et l'hygrométrie. L'éclairage indirect est réglé en intensité et répartition en évitant les reflets. Les couleurs des différents éléments sont appropriées. La salle est aussi silencieuse que possible, donc bien isolée.

V. Enseignements de l'expérience.

V.1. Enseignements tirés en France sur les tranches et sur simulateur.

Ils ont été tirés sur trois plans :

V.1.1. Difficultés de certaines phases de conduite.

Certaines phases de conduite étaient complexes pour l'opérateur ; un cas important était rencontré lors du démarrage de la tranche en situation monophasique ; aussi des améliorations ont été apportées au système et la régulation de pression primaire a été adaptée à cette situation ; des alarmes spécifiques ont été disposées.

V.1.2. Opportunité d'améliorer le traitement de l'information.

A l'arrêt, apparaissent des alarmes qui ne correspondent pas à des défauts véritables dans cette situation. Des modifications, visant à remédier à cette situation, ont été étudiées et d'ores et déjà effectuées sur les tranches de Bugey. Elles sont en cours de réalisation sur CP1.

En outre, en situation incidentelle ou accidentelle, l'opérateur se trouve en présence d'une avalanche d'alarmes (par exemple, après arrêt d'urgence ou injection de sécurité) sans qu'il puisse distinguer le défaut, cause de l'incident de ceux qui n'en sont que la conséquence. Dans ces conditions, le diagnostic de l'incident n'est pas aisé. Un traitement des alarmes est très souhaitable.

V.1.3. Opportunité d'améliorer la salle de commande 900.

L'expérience a fait ressortir les inconvénients de l'architecture CP1.

On trouve en effet :
— sur le pupitre central, les commandes nécessaires à la fois en service normal et au démarrage-arrêt,
— sur le tableau arrière, les commandes propres au démarrage-arrêt.

Ainsi, en période de démarrage-arrêt, l'opérateur est condamné à de fréquents déplacements entre le pupitre central et le tableau.

Même constatation pour les moyens d'information parfois éclatés entre pupitre et tableau.

Un pupitre tableau unique, comme il a été conçu à Fessenheim à titre exceptionnel, offre des frontières communes entre les deux zones considérées et permet ainsi plus facilement le regroupement de fonctions entières. Il se prête aussi mieux à la réalisation de synoptiques et au développement des écrans de visualisation.

V.2. Enseignements de TMI.

L'accident de TMI a révélé que l'aptitude de l'opérateur à réagir correctement en situation accidentelle pouvait se situer en deçà de celle que lui supposait généralement le

concepteur. Ce dernier a donc pris conscience qu'il était nécessaire d'aider davantage l'opérateur dans ces circonstances difficiles et que les moyens mis jusque-là à sa disposition pouvaient être insuffisants en situation dégradée. Plus précisément, des enseignements sont tirés sur les trois points suivants :

V.2.1. Amélioration de l'instrumentation.

Deux soucis se dégagent :

a) La validité des informations. Il faut ne pas confondre ordre de fermeture et information de position de fermeture d'un robinet — ce qui est évité en France — et prendre l'information sur la tige du robinet et non sur celle du servo-moteur. Par ailleurs, le champ de validité de certaines mesures doit être élargi (exemple : mesures de température cœur).

b) La recherche de mesures supplémentaires permettant d'être renseigné sur l'état de sûreté de la tranche, y compris dans les conditions dégradées : niveau d'eau dans la cuve, présence d'incondensables.

V.2.2. Amélioration du traitement de l'information, en situation accidentelle.

Là encore, il est apparu qu'il y avait trop d'alarmes, qu'il convenait donc d'inhiber celles sans signification dans une telle situation et de hiérarchiser les autres. Certains traitements devraient être effectués afin de faciliter le diagnostic de l'opérateur (par exemple : calcul de la marge à l'ébullition dans le réacteur). Un effort particulier doit également être fait dans la présentation des informations, en regroupant les informations utiles dans une telle situation, en faisant bien ressortir l'état de sûreté de la tranche.

V.2.3. Adjonction de quelques automatismes jugés nécessaires

tels que la télécommande des filtres à iode permettant d'épurer avant rejet. Il faut souligner que peu d'améliorations sont apparues possibles dans ce domaine.

Un programme très important a été mené en France après TMI. Certaines améliorations ont déjà été mises en place sur le 900, d'autres sont encore à l'étude.

VI. Evolution de la conception. Application au 1300.

VI.1. Conduite - Automatismes.

Dans l'ensemble, les mêmes principes que sur le 900 sont appliqués. Toutefois, on s'est efforcé de faciliter la conduite de la tranche, donc de réduire le nombre des organes de commande et d'accroître le niveau d'automatisme des changements d'état.

Sur la chaudière, cet effort s'est révélé assez vain et on en est resté à peu de choses près à la conception 900. Notons toutefois des modifications ponctuelles : adjonction d'automatismes spécifiques sur la fermeture des vannes d'aspersion du pressuriseur, introduction de verrouillages supplémentaires (mise en service des pompes RRA).

Dans la salle des machines par contre, un regroupement pour commande par fonction élémentaire est opéré lorsque les études fonctionnelles ne font pas apparaître d'inconvénients.

Il n'était donc pas prévu actuellement de faire évoluer de manière très sensible le niveau d'automatisme des tranches 1300 par rapport au 900.

VI.2. Information - Surveillance.

C'est le domaine dans lequel l'évolution est la plus importante

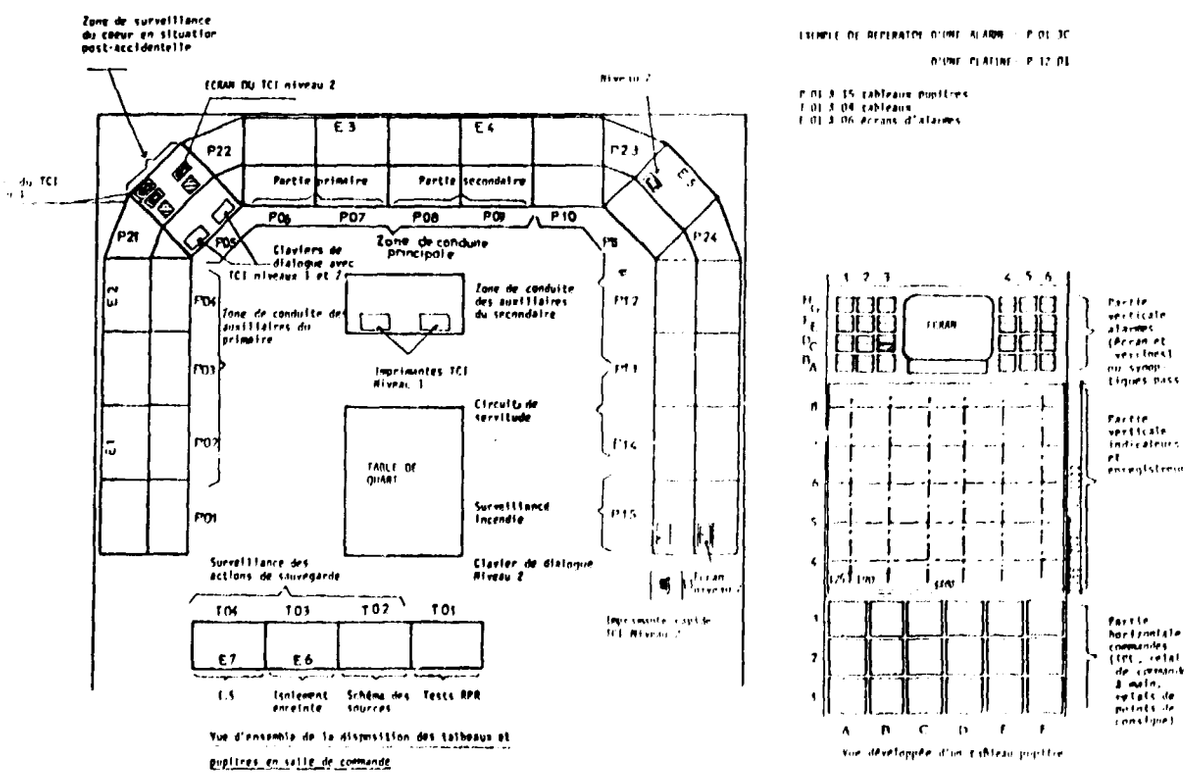
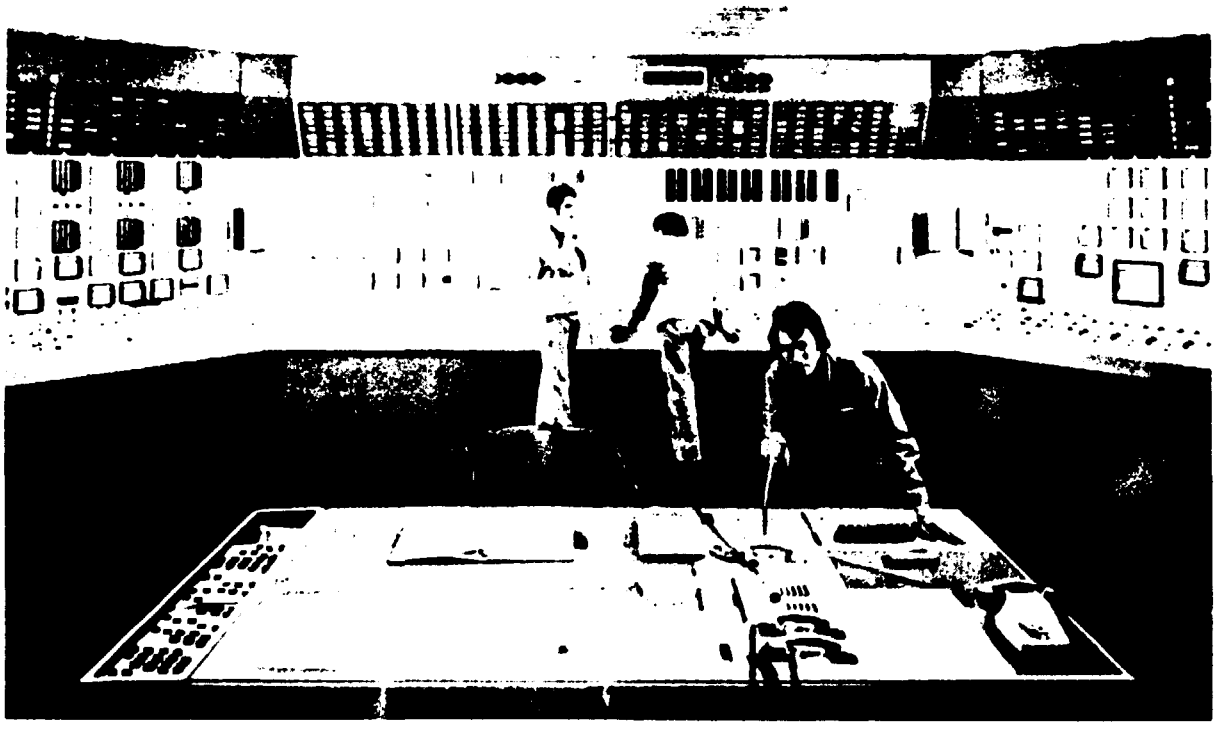


Schéma de la salle de commande 1300.



Salle de commande de Fessenheim, prototype de la salle 1300.

Elle porte sur
- l'instrumentation mise en œuvre,
- les traitements effectués,
- la présentation.

VI.2.1. Instrumentation.

Un système de surveillance post-accidentelle est étudié (application du Regulator Guide 1-97). Un effort est par ailleurs en cours, en vue de faire le développement ou d'améliorer les performances de mesures nouvelles (niveau cuve, taux de vide) pour les états dégradés. L'application aux différents paliers n'est pas définie pour l'instant.

Une attention particulière est portée à la validité des mesures (corrections, surveillance, qualification aux conditions d'ambiance). A ce titre, la comparaison des valeurs issues de capteurs redondants sera, sur le 1300, effectuée par le TCI.

VI.2.2. Traitement des informations.

L'enseignement de l'expérience conduit à mettre à la disposition de l'opérateur des informations triées et hiérarchisées. Pour cela, un effort a été fait dans trois directions :
— amélioration notable du traitement des alarmes visant à ne fournir à l'opérateur que des alarmes représentatives d'un défaut réel de l'installation et à ne lui donner que l'alarme provquée par l'apparition d'un défaut et non celles dues aux actions de sécurité initiées par ce défaut ; ainsi, en règle générale, on inhibera les alarmes signalant le dépassement d'un critère physique qu'il est normal d'avoir, compte tenu de l'état de la tranche ; en outre, lors d'un arrêt d'urgence et de l'initiation d'une action de protection, on ne fournira à l'opérateur que l'alarme origine de l'action de sécurité et l'on inhibera les alarmes conséquences de cette action,
— traitement d'aide à l'opérateur en situation normale : il s'agit, pour l'essentiel, de l'aide au pilotage visant à optimiser l'intervention de l'opérateur,
— traitement d'aide à l'opérateur en situation accidentelle.

Ces traitements consistent :
- à regrouper les informations essentielles pour la surveillance du déroulement des actions de sauvegarde,
- à tenter d'identifier, par des corrélations, la situation de la tranche vis-à-vis de paramètres vitaux, tels que le bilan d'eau primaire (il s'agit d'une application limitée de l'approche par états définie en VI.3),
- à guider l'opérateur dans son diagnostic en l'aidant, par un traitement automatique, à choisir la bonne procédure.

L'étude de ces modifications est en cours sur le 1300.

VI.2.3. Présentation de l'information.

Les particularités de la présentation des informations sur le 1300 sont notamment :
— les alarmes de catégorie 1 restent sur verrines,
— les alarmes de catégories 2, 3, 4 sont présentées sur les 7 écrans de visualisation,
— 5 écrans de visualisation couleur du TCI sont prévus.

Cette évolution dans l'usage des écrans, permettant une souplesse accrue pour la présentation des informations, devrait se développer sur N4 *(voir plus loin).*

VI.3. Approche par états.

Les procédures de conduite post-accidentelles actuelles sont rédigées à partir de l'étude de séquences types.

La procédure initiale d'aide au diagnostic consiste à identifier, d'après l'évolution de paramètres significatifs, le type d'accident de façon à utiliser la procédure post-accidentelle correspondante. Cette approche est rendue difficile parce qu'il n'est pas possible d'envisager de manière exhaustive tous les scénarios possibles d'accident en incluant notamment d'éventuelles erreurs d'opérateurs ou des défaillances de matériels.

Une autre approche (dite approche par états), actuellement en cours d'étude, a donc été envisagée dans le but de fournir à l'opérateur les actions à effectuer, en fonction uniquement de l'état de l'installation, indépendamment du type d'accident, de défaillances de matériels ou d'erreurs éventuelles de l'opérateur dans la phase initiale. Elle offre donc à l'opérateur le grand intérêt d'une possibilité pour

lui de rattrapage, lorsqu'il n'a pas su, comme à TMI, identifier sa séquence accidentelle.

Cette approche consiste à effectuer un recensement exhaustif des états thermodynamiques de la chaudière à partir des modes de circulation du fluide (circulation forcée ou naturelle), des états du fluide (monophasique ou diphasique) et des bilans de masse, d'énergie et de quantité de mouvement.

Ces états, caractérisés par un nombre réduit de paramètres physiques (pression primaire, température primaire, marge de sous-saturation ou monophasique...) étant connus, on peut alors spécifier à l'opérateur les actions à entreprendre pour stabiliser la chaudière dans un mode de refroidissement (par exemple, en augmentant ou diminuant l'inventaire en masse) ou la ramener dans un autre mode jugé plus sûr.

Dans le cas où les moyens à mettre en œuvre ne seraient pas disponibles, l'installation évoluerait vers un autre état pour lequel des actions, dites ultimes, seraient de même spécifiées.

Cette approche, complémentaire à celle utilisée actuellement, nécessite toutefois la mise en œuvre d'une instrumentation supplémentaire (inventaire en eau dans la cuve, taux de vide dans les branches chaudes...) pour caractériser sans ambiguïté les différents états en situation très dégradée.

Il y a, aujourd'hui, un bon espoir de mener à bien cette approche prometteuse vis-à-vis des problèmes de fiabilité humaine en situation accidentelle.

VI.4. Conception générale de la salle de commande.

Un effort est fait pour moderniser la salle de commande, en améliorer la présentation par une meilleur ordonnance des moyens de commande et de contrôle, par un recours plus grand aux équipements évolués de « Hardware » et regrouper les moyens nécessaires, en particulier, en situation accidentelle.

La salle de commande 1300 comprend, comme celle de Fessenheim, un grand tableau pupitre et un tableau arrière regroupant tous les moyens de conduite et d'information associés.

Pour le regroupement satisfaisant des moyens relatifs à une même fonction, les matériels sont regroupés en zones de conduite différentes de celles de CP1. Une zone de conduite principale proche d'une zone de surveillance du cœur en situation accidentelle regroupe tous les moyens nécessaires :
— au réglage de la charge (régulation turbine, alternateur),
— au réglage de la puissance neutronique,
— au réglage de la pression primaire,
— à l'alimentation du générateur de vapeur (normal et secours),
— au réglage du débit de contournement de la turbine,
— à l'arrêt d'urgence et au déclenchement turbine.

VII. Evolution future. Palier 4.

Les délais d'exécution du palier 1300 actuel n'ont pas permis de tirer tout fruit des enseignements de l'expérience. Aussi pour le palier futur, nommé palier N4, une réflexion globale est entreprise visant à adapter le contrôle-commande et la salle de commande aux nouveaux concepts d'exploitation, dans les différentes situations normales, accidentelles, post-accidentelles.

Le point de départ de cette réflexion est une analyse fonctionnelle basée non plus seulement sur les données de systèmes élémentaires comme autrefois, mais aussi sur les procédures de conduite, fiches d'alarmes et les aptitudes de l'opérateur telles qu'elles découlent de l'expérience d'exploitation acquise tant en centrale que sur simulateur.

Le but de cette analyse est d'identifier les différents traitements d'aide à la conduite, de corrélations de données à développer et les différents éléments à prendre en compte dans la conception de la salle de commande.

Un simulateur d'étude sera commandé, qui permettra de programmer et de mettre au point les traitements et corrélations précités et de valider la conception d'ensemble de la salle de commande. Enfin, une étude technologique, visant à adapter les matériels existants aux besoins définis, à simplifier les interfaces, à standardiser les échanges d'informations, est également lancée.

Cette réflexion fait largement appel à tous les moyens d'EDF. Le constructeur Framatome y est associé.

Cette étude lancée en octobre 1980 devrait se terminer en 1984

VIII. Conclusion.

Le retour de l'expérience a mis l'accent sur la prise en compte du facteur humain dans la conception des centrales nucléaires. Des études importantes ont été entreprises tant chez le constructeur qu'à EDF, en vue d'apporter aux tranches françaises les améliorations souhaitables dans ce domaine. Ces études sont longues à se concrétiser ; ceci résulte de leur complexité, de la nécessité, aussi, de faire des analyses approfondies avant de tirer des conclusions pour éviter que ces dernières soient inadaptées, enfin de la difficulté rencontrée dans la gestion de ces améliorations applicables à de nombreuses tranches dans tous les états d'avancement possibles depuis l'avant-projet jusqu'au service industriel.

* *
*