New concepts in control-room design

Worldwide, more attention is being given to improving the man-machine interface

by J. Furet

Since the beginning of the 1980s, the role of human factors in nuclear plant instrumentation and control has taken added emphasis, mainly because of the Three Mile Island accident and advances in data processing, display equipment, and automatic programmable devices. TMI clearly showed that operators can be burdened by "information overload" and that more attention had to be given to the human element and actual operating experience.

In the following article, Mr Furet summarizes major steps that have been taken, and are being planned, around the world to improve the man-machine interface for safe and economic nuclear power generation.

Since the end of 1979, measures related to the man-machine interface that have been implemented worldwide – particularly in France, Japan, and the United States – have many features in common. These measures were taken after ergonomic evaluation and analysis and particularly relate to the layout of control consoles and panels, safety parameter display systems (SPDS), emergency operations facilities (EOF), technical support centres (TSC), new instrumentation, and procedures.

In some cases, however, present regulations still are delaying the utilization of computerized and advanced technologies important to improving the man-machine interface. For example, the use of multiplexing techniques for electric signal transmission – which can decrease risks from fire and loss of leak tightness in the reactor building by reducing the number of electric cables and penetrations – is prevented by present rules, such as physical and functional separation criteria for redundant equipment and channels. It would therefore be reasonable to suggest that regulations should be more speedily adapted to the use of new technologies.

Moreover, the new technologies used in electric signal transmission, data acquisition, processing and display, and standardization of monitoring and control devices also can help improve system reliability and availability, as well as lower potential dangers.

Mr Furet is Service Head, Commissariat à l'Energie Atomique (CEA), Institute of Technological Research and Industrial Development, Department of Electronics and Nuclear Instrumentation. This article is adapted from a summary of his extensive review, *Conception des salles de contrôle-commande interface homme-machine pour la conduite et la surveillance des centrales nucléaires.*

Layout inside the control room

The importance of ergonomic evaluation of the control room was recognized very quickly by plant operators.

In France, an ergonomic analysis of the 28 identical pressurized-water reactor (PWR) units under the CP-1 and CP-2 programmes of Electricité de France (EdF) resulted in construction of a full-scale mock-up of the control room. This mock-up was then used to study proposals for modification and improvements in the layout of panels in collaboration with operating teams from different power plants. Thereby, it was possible to make maximum use of on-the-job experience gained by operators (amounting to a total of 35 years), their ideas, and also the errors made by them.

As a basis for determining modifications or improvements to be made on the mock-up, 20 principles of layout were selected. The modifications and improvements that were finally chosen necessitate a complete change in the horizontal panels of the front control console and those of the back control board. Putting these modifications into effect in all the 28 PWR units will take through 1986.

Safety parameter display system (SPDS)

Of the operator aid systems, the SPDS was studied on a priority basis. In the United States, the Nuclear Safety Analysis Center (NSAC) of the Electric Power Research Institute (EPRI) produced a preliminary design of the most characteristic parameters for plant behaviour in pre- and post-accident situations during its study of the TMI accident.

Control room at TMI-2. (Credit: J. Furet, CEA)

Safety Parameter Display System

Alarms		Critical safety functions
Nuclear power reactivity	HT	Reactivity
Primary coolant pressure	HT	
Primary coolant pressure	LT	
Pressurizer level	LT	Primary
Air activity in condenser vacuum system	HT	Coolant
		Integrity
RB air filter activity	HT	
RB pressure	HT	
RB sump level	HT	
Saturation margin	LT	
Thermal shock (PT)		Core
Saturation margin trajectory	LT	Heat
Pressurizer level	HT	Removal
Core heating	HT	
Core cooling	LT	
Core outlet temperature	HT	
Steam pressure	HT	
Steam pressure	LT	Heat Removal by
Steam generator water level	LT	Secondary System
RB pressure	HT	Reactor Building
RB activity	HT	Integrity

Notes: HT = high threshold, LT = low threshold, RB = reactor building

There have since been several SPDS designs for different types of nuclear steam and supply systems. Their study and development have sometimes been made more complicated by problems of software qualification and the earthquake resistance of the hardware, especially in Japan and the United States.

The first SPDS put into operation was the one designed by NSAC for the old Yankee Rowe plant, which was equipped with the first PWR used for electricity generation in the USA and which had a large proportion of operators who had been working at the plant for more than 20 years. It is described in the above table.

Technical support centre

The technical support centre (TSC) generally is situated near the instrumentation and control room, in a room in the electrical building, or even at the visitors entrance, with a direct view of the control room. Sometimes it is located in a specially constructed building near the turbine hall.

The TSC and facilities for data acquisition, processing, and display vary greatly in importance. An example of the most up-to-date TSC is the one at the Trojan nuclear power plant operated by Portland General Electric Company in the USA. There, it was necessary to build a separate facility where the visual display room and the computer room occupy an area of about 80 square metres. It has 17 offices for the emergency management team.

At the Trojan TSC, process signals are handled by three computers that also are used for processing data from the SPDS and any data available at the emergency operations facility. Two of the three computers are needed to ensure all necessary functions. All signals are stored on tape for 24 hours and then transferred to disc. A fast printer delivers part of these signals on request, and there are 20 telephone lines for communication between the TSC and the control room, the EOF, and the US Nuclear Regulatory Commission (NRC) at both the regional and national level.

New instrumentation

New instrumentation includes new sensors, associated electronic sub-assemblies for measuring purposes, and data processing hardware. The corresponding equipment is installed on the nuclear steam supply system and the reactor building hardware. Examples of new sensors are those used for evaluating the gamma activity over a measurement range of the order of 10^6 in the reactor building and for determining the water level in the reactor vessel above the fuel elements.

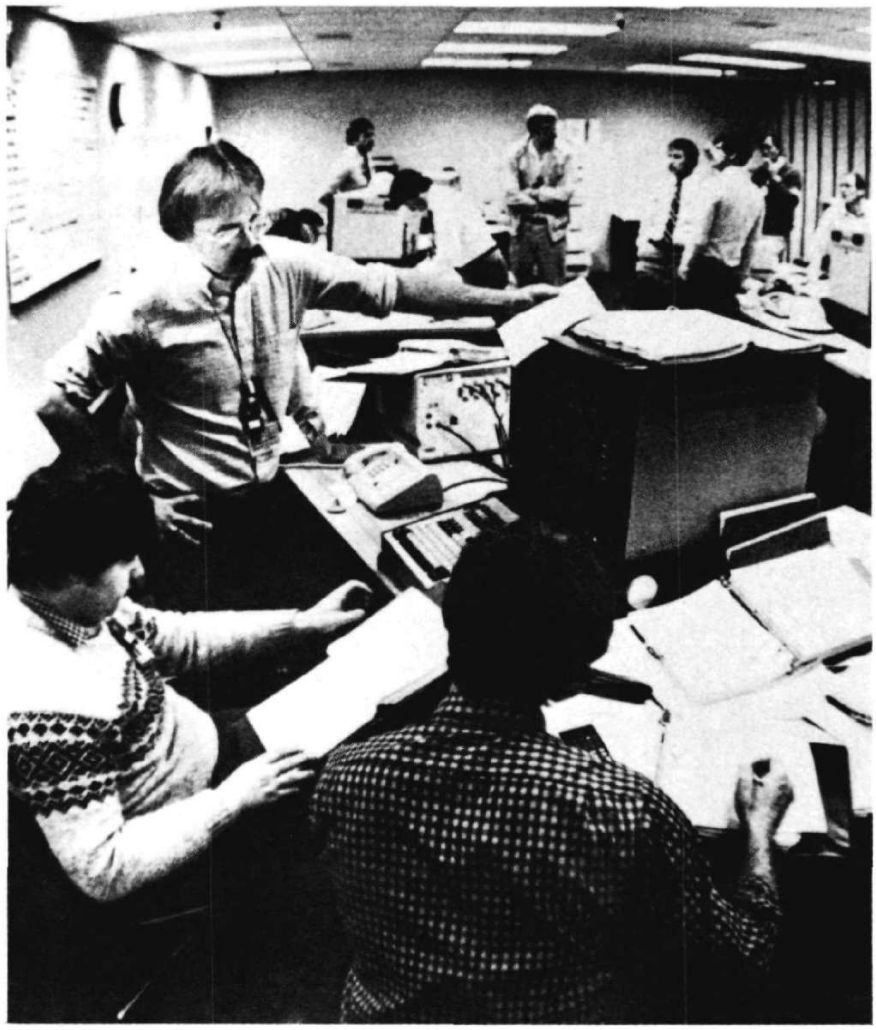
Regarding the additional data processing hardware, mention should be made of the core cooling monitor used to measure the pressure and temperature saturation margin. Most of the time this instrument uses a microprocessor that calculates the saturation margin from the primary pressure, hot- and cold-leg temperatures, and coolant temperatures at the outlet of the fuel subassemblies.

Procedures

Procedures at the disposal of operators constitute the most important component of the man-machine interface since they hold fundamental implications for the operator's response in the event of accidents.

Since 1979, emergency procedures have no longer been based solely on the event-oriented approach. Instead, a status-oriented approach has been developed. This approach usually calls for the design of a complex logic diagram and is more efficient in cases of operator error in diagnosing an initiating event, or in the case of simultaneous occurrence of several initiating events.

Procedures based on the event-oriented approach, which are sequential, are easier for operators to apply. Therefore, the status-oriented procedures are still used by the shift technical advisor (STA), who advises the operational team.



A full-scale emergency exercise at Trojan puts the plant's technical support center (TSC) to work. Engineering personnel (foreground) review reactor conditions to determine corrective actions. Trojan's TSC, once a part of the plant's emergency operations facility, is now a separate, on-site facility. (Credit: INPO)

In France, the strategy applied since 1979 by EdF uses a procedure that is based on the status of core cooling and availability of the engineered safety systems. It is applied by the safety and radiation protection engineer (ISR), enabling him to keep permanent watch over the plant and, if necessary, to instruct the operator to start safety injection and to operate the containment spray system. By so monitoring changes in the plant cooling status, he can even advise discontinuation of the procedure being applied.

Steps now being taken to further improve procedures available to operators relate to systematic diagnosis of deteriorated cooling status and formulation of corresponding corrective actions to prevent or limit core damage. An important step in the developing emergency procedures is validation on simulators. Improvement of specific simulators is still needed for the simulation of long-duration transients and the behaviour of the core in case of significant damage.

R&D activities requiring emphasis

Areas of prime importance to research and development relate to validation of sensor signals; processing, filtration, and classification of alarms; overall evaluation of plant status; data processing and display; periodic tests, bypass of signals and trips, and locking of actuators; and adaptation of regulations to the use of new technologies.

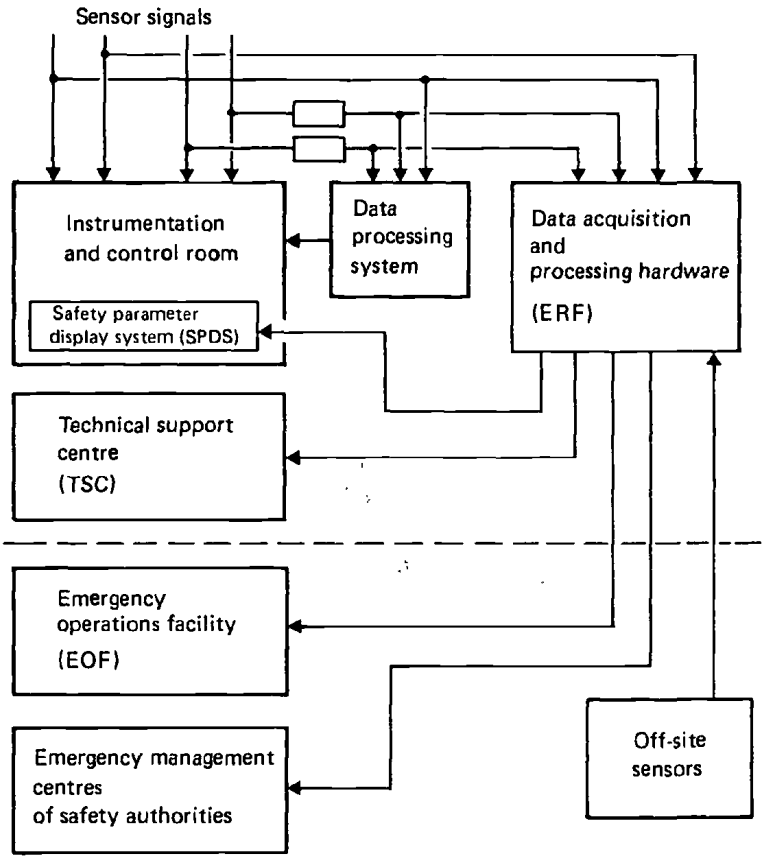
Validation of sensor signals

Measurement and position sensors for actuators, such as valves, electrical switches, circuit breakers, and so on, play an essential role in the man-machine interface – especially since operators can get the "feel" of the process only through signals transmitted by sensors. Validation of these signals has to be improved by increasing the reliability of sensors and by making better use of the redundancy of the associated measurements, which can most often reveal a faulty sensor.

Additionally, a faulty sensor can be located with certainty by means of relatively simple processing to correlate signals from sensors measuring different physical variables. Finally, on-line verification of specific characteristics, such as the response time of the sensor and the noise level of the signal associated with the measurement, can ensure satisfactory operations.

This continuous signal processing and periodic verification of characteristics should be further developed and implemented for most sensors, regardless of their

Emergency management and response: Structure and information flow



Operating experience clearly shows the marked effect of operator behaviour and actions on plant availability and nuclear safety. This chart of selected accidents illustrates that in regard to the man-machine interface elements of instrumentation, procedures, and operator behaviour, the summary observations for each accident are very similar.

Plant	Power (MWe)	Year	Component involved	Period of non-availability	Instrumentation	Procedures	Operator behaviour
Windscale	—	1956	Fuel	Decom-missioned	Unsuitable	Very imprecise	Errors in interpretation
Enrico Fermi	150	1966	Fuel	4 years	Malfunctioning	Very imprecise	Errors in interpretation; delay in action of 15 minutes
St Laurent A1	460	1969	Fuel	1 Year	Unsuitable	—	Errors in interpretation
Browns Ferry	2 X 1067	1975	Instrumenta-tion and control	1.5 years	Major failure	Incomplete	Very good reaction; Serious accident avoided
TMI-2	880	1979	Fuel	Indefinite	Unsuitable	Imprecise	Errors in interpretation; inadequate action
St Laurent A2	515	1980	Fuel	2 years	Partly unavailable	Incomplete	Errors in interpretation

purpose. Priority should be accorded to those used in the instrumentation of the protection system or associated with some controllers.

Alarm processing, filtration, classification

In a typical 900 to 1000-megawatt unit, the number of alarms is on the order of 1000 to 1500. During a loss-of-coolant accident (LOCA), or one of that type, several hundred alarms may occur in the first two minutes at a frequency of as high as 20 to 30 per second. Obviously, operators cannot respond to them all at the same time, nor can they sift or classify them in order of importance. Yet such mental operations are essential to gain an understanding of the overall unit status.

It is surprising to find that at virtually all operating facilities the problems of coding, filtering, and grading alarms have not been better grasped and handled. Activities planned in this area should be given perhaps the highest priority to improve this situation, since it represents one of the most important diagnostic aids for operators in case of accidents.

In operating facilities using wired alarm sub-assemblies and assemblies, changes can be relatively difficult or costly. This may explain, though not justify, the attitude of plant operators who tend to plan such improvements for the medium, or perhaps long term, when immediate measures actually ought to be taken to improve an unsatisfactory situation.

Evaluation of plant status

Currently, operators gain an overall picture of the plant status with the help of panels on which information usually is displayed in analog form. This enables them to see the state of functions and systems important to safety. However, this geographical scattering of useful information can prevent the operators from making a rapid overall evaluation, which is vital in the event of an accident and for selecting proper emergency procedures.

It is possible to make a quick evaluation by examining a limited number (up to 30) of physical variables or parameters. Therefore, even in cases where automation of instrumentation would be highly developed, location of the SPDS in the control room will continue to be essential. SPDS undeniably is one of the most effective ways to evaluate the plant's overall status, and it is a diagnostic aid as well. Its design, now based on critical safety functions, undoubtedly will evolve as more operating experience is gained.

It must be added, however, that overall evaluation of the status of functions important to safety is not enough if an incident occurs. It has to be supplemented by the overall evaluation of systems status and components, namely the protection system, engineered safety systems, power supplies, compressed air supply, and the heat sink. At present, data stemming from these systems and components are both dispersed and incomplete.

Data processing and display

Advances in data processing equipment (digital computers, associated interfaces, colour display screens) have considerably improved the processing and display of information in the instrumentation and control room. Calculation speeds and memory capacities of the current generation of computers are fully compatible with the acquisition and processing speeds needed for the analog, digital, and on-off signals used for monitoring and control. These signals may rise to as many as 20 000 in the future.

The graphic and colour resolutions of the display screens allow a high degree of versatility for numerical data, curves, texts, diagrams, and for the overall display picture of the plant status.

In data processing and display development, it is advisable to take into account the sequential operation of the computers and the ability of operators to memorize information, which may be somewhat limited. To offset this, facilities for dialogue with computers should be provided so that, regardless of plant status and computer operations being performed, the operators can have rapid access to desired data, as well as to data files and trends.

Greater use should be made of displaying data on colour screens by images that give the operators an overall, as well as detailed view, of plant status. This kind of display, which so far has been rarely used in control rooms, requires a thorough study of the strategy of visual display and operator dialogue. Additionally, a hierarchical structure for the display should be established and tested on a simulator.

Periodic testing

Periodic tests now are often carried out manually. In the case of assemblies or sub-assemblies of systems important to safety, they mostly require bypass of signals and locking of actuators in order to avoid inadvertent triggering of protection or engineered safety systems. During performance of such tests, the functions carried out by safety systems should, of course, be maintained.

Operating experience shows that a significant number of cases during periodic testing involve inadvertent activation of protection and engineered safety systems. Apart from their impact on plant availability, such actions may give rise to incidents, such as those from inadvertent safety injection. These are mainly due to operator error and may be attributed to:

- The format of test procedures, which are not worded in a uniform manner and are therefore difficult to apply because of the diversity of equipment
- Imprecise test ranges
- Operation of bypass signals, trips, and locking of actuators without taking into account the unavailability of redundant equipment.

The probability of "operator errors" can be reduced by partial or total automation of periodic tests and centralization of monitoring and control devices in the control room; additionally, bypass and locking can be greatly facilitated. Preferably, such automation and centralization should be put into effect quickly so that improvements in overall evaluation of plant status can be gained as well.

Past efforts, recommendations

Well before the TMI accident, research and development had focused on instrumentation and control and the man-machine interface.

In France, development activities were concerned with equipment based on new microprocessor technology — namely electronic relay devices with programmable logic (CONTROBLOC) and the numeral integrated protection system (SPIN). Development of surveillance and fault-diagnosis systems was geared towards detection of leaks and migrating material in the primary circuit, and to evaluation of the vibrational behaviour of the components of the primary circuit and the turbo-generator group.

In the United States, the four nuclear steam supply system manufacturers had designed and proposed new advanced control rooms, even though instrumentation and control generally are designed by industrial architects and construction is diversified even among units of the same type and at the same site. Some of the new control rooms have been built, such as those made by Babcock & Wilcox and General Electric. GE was the first company, in the early 1970s, to launch an "advanced control room" programme, which led to the development of the "NUCLENET 1000" system.

Regarding operator aids for surveillance and diagnosis, the Electric Power Research Institute (EPRI) had started the DASS programme as early as 1976. The diagnostic methodology was based on the use of cause-and-consequence diagrams, but the system never came to be applied directly in any US nuclear plant. EPRI also had a programme for the evaluation of control rooms from the standpoint of human factors. Conclusions from it closely matched recommendations that were made by the Kemeny Commission following the TMI accident.

In Japan, programmes initiated in the early 1970s stand behind today's activities by the three manufacturers — Mitsubishi, Hitachi, and Toshiba — for developing new control-room hardware and instrumentation.

Perhaps the most consistent and long-lasting programme in the pre-TMI period was the one put into effect by teams working on the Halden Reactor Project of the Organisation for Economic Co-operation and Development (OECD). As far back as 1967, an active team of scientists initiated studies relating to nuclear power plant instrumentation and control on the basis of experience accumulated in reactor dynamics and in-core instrumentation techniques. Initially, the main purpose of these studies was to apply modern theories of control to nuclear power plants with the use of digital computers.

In the mid-1970s, these studies were re-oriented. They now dealt with the design of operator aid systems for surveillance and diagnosis; the operator's role and behaviour in avoiding and limiting the consequences of incidents; the improvement of communication between operator and machine; and the improved reliability of the software and hardware for control systems based on digital computers.

On an international level, recommendations for future actions following the TMI accident were summed up in the September 1980 report *Adaptation of Nuclear Safety Research Programmes After the Three Mile Island Accident*, published by the OECD. In one section, the report covers reactor instrumentation, data recording and display, control-room design, formulation of emergency procedures, human behaviour, and research on simulators and operator training.

These recommendations undoubtedly were based to a large extent on those proposed in the US. Major recommendations made by the US Nuclear Regulatory Commission (NRC) relating to instrumentation and control and the man-machine interface were:

- Evaluation and analysis of instrumentation and control-room design from the standpoint of human factors
- Installation of new instrumentation to measure the water level in the reactor vessel above the fuel assemblies; monitor core cooling for measurement of the saturation margin; measure continuously the water level in the containment sumps; measure temperature and humidity; measure hydrogen concentration; and measure activity deriving from gamma radiation
- Installation of a safety parameter display system (SPDS) in the control room, a technical support centre (TSC) near the control room, and an emergency operations facility (EOF) near the power plant
- Installation of communication devices for transfer in real time of significant information on the plant status to emergency centres of the safety authority.