ORGANISATION FOR ECONOMIC
CO-OPERATION AND DEVELOPMENT

NUCLEAR SAFETY DIVISION

STEERING COMMITTEE FOR
NUCLEAR SAFETY

RESTRICTED

Paris, drafted: 24-March-93
dist.: 19-Nov-1993
OLIS: 23-Nov-1993

NEA/CSNI/R(93)18

Orig. Eng.

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

PRINCIPAL WORKING GROUP N°1 EXPANDED TASK FORCE ON HUMAN FACTORS

TASK 3: "NEW MAN-MACHINE INTERFACES IN NUCLEAR POWER PLANTS"

PART I: EXECUTIVE SUMMARY AND SUMMARY OF REPORTS

November 1993

NEA/CSNI/R(93)18

OECD

NEA

TASK 3: "NEW MAN-MACHINE INTERFACES IN NUCLEAR POWER PLANTS"

PART I

Executive Summary and Summary of Reports

Prepared by Experts from Principal Working Group N°1
Expanded Task Force on Human Factors
of the Nuclear Energy Agency
of the Organisation for Economic Cooperation
and Development (OECD)

November 1993

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS
OECD NUCLEAR ENERGY AGENCY
Le Seine St. Germain - 12, Boulevard des Iles,
F-92130 Issy-les-Moulineaux
Tel: (33-1) 45 24 82 00 Fax: (33-1) 45 24 11 10
Electronic mail: NEA@FRNEAB51

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The Committee on the Safety of Nuclear Installations (CSNI) of the OECD Nuclear Energy Agency (NEA), is an international committee made up of senior scientists and engineers. It was set up in 1973 to develop and coordinate the activities of the Nuclear Energy Agency concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations. The Committee's purpose is to foster international cooperation in nuclear safety among the OECD Member countries.

The CSNI constitutes a forum for the exchange of technical information and for collaboration between organizations which can contribute, from their respective backgrounds in research, development, engineering or regulation, to these activities and to the definition of its programme of work. It also reviews the state of knowledge on selected topics of nuclear safety technology and safety assessment, including operating experience. It initiates and conducts programmes identified by these reviews and assessments in order to overcome discrepancies, develop improvements and reach international consensus on technical issues of common interest. It promotes the coordination of work in different Member Countries including the establishment of cooperative research projects and results to participating organizations. Full use is also made of traditional methods of cooperation, such as information exchanges, establishment of working groups, and organization of conferences and specialist meetings.

The greater part of the CSNI's current programme of work is concerned with safety technology of water reactors. The principal areas covered are operating experience and the human factor, reactor coolant system behaviour, various aspects of reactor component integrity, the phenomenology of radioactive releases in reactor accidents and their confinement, containment performance, risk assessment, and severe accidents. The Committee also studies the safety of the nuclear fuel cycle, conducts periodic surveys of the reactor safety research programmes and operates an international mechanism for exchanging reports on safety related nuclear power plant accidents.

In implementing its programme, the CSNI establishes cooperative mechanisms with NEA's Committee of Nuclear Regulatory Activities (CNRA), responsible for the activities of the Agency concerning the regulation, licensing and inspection of nuclear installations with regards to safety. It also cooperates with NEA's Committee on Radiation Protection and Public Health and NEA's Radioactive Waste Management Committee on matters of common interest.

EXECUTIVE SUMMARY

The present document summarises the reports provided by the member countries reflecting the actual status of consideration of Human Factors principles for the nuclear power plants. The report has neither been intended as a state-of-the-art report nor as a complete review. It is mainly concentrated on the Human Factors, even if problems related to hardware and software reliability have not been neglected since they constitute a major issue in several countries.

The adoption of Human Factor principles, in conjunction with the availability of advanced digital technology, has already led to the addition of computerised operator aids to almost all the operating plants in the member countries and to the study and the design of fully digitized control rooms for the future plants in some of them.

As regards the licensing issue, many uncertainties still exist on the methodology and tools to be used and no internationally accepted standards have been established by now, especially for the software to be used in safety systems of nuclear power plants. The licensing of Man-Machine Interfaces (MMIs) is, in conclusion, at the very beginning of the process as in the past not enough attention has been given to human factor and software licensing aspects. In some countries the preparation of new "ad hoc" guidelines, or the updating of the existing one for digital equipment, are under way. Several examples of licensing of MMIs in countries where control room systems are safety classified, are described in the report highlighting the different approaches adopted.

The evaluation/validation phase is another very important aspect of the implementation process of MMIs, to assure its complete compliance with the design requirements. This phase is performed in various countries following different approaches ranging from the compliance with existing standards up to the extended use of "ad hoc" simulators and mock-ups.

One of the major issues in MMIs design is the provision of advanced alarm system supporting the operator in his supervisory tasks and avoiding at the same time the problems related to information overload that are typical of the existing alarm systems. Several examples of improved alarm system implementation and existing alarms system evaluation are presented. They are based upon concepts such as subdivision of the alarms in functional groups, adoption of filtering criteria, use of priority codes, cut-out conditions, variable limits.

The use of Artificial Intelligence under the form of Expert Systems is another opportunity made available by the modern digital technology. Expert Systems can be applied to several areas of plant supervision and control such as real time diagnostics, decision support, emergency response in order to enhance operator understanding of the plant status in whatever situation and therefore to help him in the operational decision-making process.

The proper balance between automation and human actions is certainly one of the major issues in designing nuclear plant as it heavily affects both safety and reliability of plant operation. The availability of advanced digital technology allows the allocation to the machine or more and more complex functions and it is credible that the automation level in plant operation should increase in the future, even if that will not necessarily cause an increase in plant safety. The complexity of this task is also illustrated by the wide spectrum of solutions adopted in various countries. More time should be devoted to evaluating the optimum in task allocation, an evaluation should be done between engineers and human factor specialists. Experience shows that good solutions may be found with very different approaches even if the industry feels a need for development of a more systematic one, starting from the definition the operator role and the operator

capability. An example, dealing with the case of advanced reactors with passive safety systems, where the operator role will change from that of a "fast actuator" of the traditional plants to that of an "intelligent supervisor", is reported.

Finally, a strong need for a human factor evaluation process for systems based on the new technologies is felt by licensing authorities, vendors and utilities. Since a wide spectrum of evaluation techniques exists, the method to be used strongly depends on the purpose of the specific evaluation. Large emphasis has been put on performing large-scale, realistic operator experiments on full-scale simulators. The results of the evaluation, that can last several years, allow to analyse in detail all the advantages/drawbacks of the chosen solutions before the actual implementation of the control room.

Other approaches, employing less resource-demanding analytical methods such as operator interviews and questionnaires, need also to be investigated.

SUMMARY OF REPORTS

Chapter 1

Main Features, Evaluation and Licensing of New Man-Machine Interfaces (MMIs)

This chapter is subdivided into three main sections dealing respectively with the main advanced features of modern control rooms and with their licensing and evaluation aspects. It is important to note that a wide spread exists in member country contributions, ranging from the addition of computerised operator aids (e.g. safety parameter display system: SPDS) to completely digitised control rooms.

This is essentially due to the fact that radically innovative solutions can be only applied at plant design level, while for plants already in operation only the addition of limited purpose advanced systems, to help the operator in some specific areas, is conceivable.

The addition of an SPDS has already been achieved for all the U.S. operating plants and similar solutions have been adopted also in many other plants world-wide (e.g. Spain, Sweden, Finland) to provide support for the control room crew, especially for the on-call safety engineer, in managing complex transients and emergency situations through a better and more immediate use of the emergency operating procedures.

Recurrent characteristics are the identification of a limited number of critical safety functions (e.g. reactivity control, core cooling, containment integrity) the normality of which indicates the integrity of the relevant plant safety barriers, the use of colour coding (from green to red) to provide operators with a straightforward indication of the challenge severity and the use of a multilevel hierarchy going from an upper level set of information down to the most detailed data.

Other important characteristics of the SPDS are certainly the concise and continuous displays, the high reliability, the importance of a feedback from operators, as regards the content and the ergonomics aspects of the displays.

Apart from the use as SPDS, advanced systems have been applied in other sectors of operator aid, for example, in the monitoring of core performances or in the presentation to the operators of synthetic data regarding the plant process status.

As a significant application in this field, it is to recall the real time core analyser (VERONA) that has been in operation in the Hungarian plants during the last 8 years, furnishing a valid support to the operator in the complex task of optimising core performances while keeping all the operational core parameters within the safety limits, visualising existing margins under the form of colour-coded core maps. An improved version of this system, performing also the SPDS function, will enter in operation in September 1993.

As a further example of operator aids, the computerised process information systems (PRINS-PRISCA), added to the most recent German plants, are reported. It is a human factor centered, fully redundant, distributed, real time computer system with full graphic capabilities and standardised pictorial symbols. Its main capabilities are related to signal validation, status displays, trend curves, overviews. Two hundred different formats are available to the operators to monitor process details on several Cathod Ray Terminals (CRTs). Another important use of advanced systems in Instrumentation and Control (I&C)

systems is related to their application in the RPS; as an example, the use of digital arithmetic modules (DAM) in the RPS of the Mulheim-Karlich plant is described (see also the "licensing of MMI" paragraph).

As regards to the addition of computerised information systems, a major application (PIS - Process Information System) has been carried out at the Krsko nuclear plant (Slovenia) where 12 new terminals were located in the Main Control Room (MCR) to display process state information. The system, based on an open three level hierarchical architecture, has the main target of presenting the operators with the necessary information both in normal and abnormal conditions (flow diagrams, dynamic component symbols, deviations from optimal conditions, etc.).

The case of the UK plant Sizewell B, presently in the final construction phase, is another example of advanced technology use for plant monitoring. It can be considered as a hybrid control room in the sense that it is a combination of computer generated displays and "conventional" mimic and control panels. In particular, for the alarm system both digital and hard-wired annunciators coexist, leaving to the former the aim to tabulate, both on affected system mimics and in tabular form, all the alarms and to the latter the aim to recall the most significant alarms on a conventional dedicated annunciator panel. Plant manual controls are however maintained hard-wired, incorporated in panels positioned around the walls of the control room. The monitoring of critical safety functions is achieved by means of computed generated display formats, with alternative seismically qualified plasma displays or hard-wired instruments, all related directly to emergency operating procedures.

The final step necessary to pass to a completely digitised control room has been made in the French plant of Chooz B where all the monitoring, control and protection functions are performed by the operators through workstations provided only with CRTs, plasma screens, track balls, keyboards, etc. Two workstations are assigned to plant operators, other two are for the shift supervisor and the safety engineer. A large animated, wall-mounted mimic, reporting the status of the main primary and secondary systems, directly linked to the field, is added to maintain a set of important information available, even in case of a common mode of failure affecting all the workstation computers. It is important to note that both an auxiliary panel, from which the operator using conventional controls and instruments can bring the plant into safe shutdown conditions, and several push buttons for the actuation of important safety functions are also provided.

For future plants, a choice in favour of fully digitised control rooms seems however a decision already taken in several other countries; it is clear that this can mean also an impact on the operator role and the level of automation: it is in fact easier to attribute a supervising role to operators and to increase the automation level in an informatised control than in a conventional one.

In Germany, on the basis of the experience gathered with the PRINS/PRISCA system, already described, and of that coming from the completely digitised control room of the coal-fired power plant of Staudinger 5 in operation since 1992, a proposal has been made to use fully digitised control rooms also for future nuclear plants.

In the U.S., the designers will incorporate critical safety functions as an integral part of the control room information display system displays. Also in this case future control rooms should present a number of workstations from which the operators will monitor and control the plant process and a large overview wall display with fixed plant process mimics to show high level plant status information to the operators.

Finally in Italy, where despite the nuclear moratorium a research program on future nuclear designs is well underway, established design criteria envisage the use of a control room very similar to the N4 type, stressing at the same time the necessity for a change of operator role as regards plant safety, in particular

introducing the concept of a significantly longer grace period (24-72 hours) for operator actions, related to the fission product containment function.

It is interesting to note that, generally speaking, in case of a common mode of failure of all the workstations, the addition of a limited-scope conventional panel in the control room is envisaged to allow operators, in any case, to manually bring the plant into safe shutdown conditions.

In Italy due to the longer grace period required for the operator actions, a further automatic back-up to the actuation of safety systems has been deemed necessary; it will be constituted by a system, completely diversified and separated from the main computerized one, based on LADDIC technology, also utilised with similar purposes at Sizewell B plant.

1.2. Licensing of Man-Machine Interface (MMI)

Even if it is always difficult to synthesise different complex situations, an assertion valid in general is possible as regards the licensing of MMIs; licensing of MMIs is still at the very beginning of the process, while the licensing process is much more developed and firm as regards the hardware and software, especially as regards their reliability. In the human factor area quite different situations have been highlighted by members, ranging from the existence of formal licensing requirements and the direct intervention of the regulator in the evaluation phase, to the application of standards left to the utility with the evaluation phase performed by an independent engineering firm.

The initial U.S. regulatory requirements for SPDS reviews, including the incorporation of accepted human factors principles were provided in NUREG 0737 and its Supplement 1. Present U.S. regulatory criteria for MMI design are contained in some sections of NUREG-O800, while only limited guidelines for reviewing advanced digital technology are contained in NUREG-0700. The need for a new guidance for reviewing MMIs where advanced control rooms, originated by NUREG-5908, presently in draft, that will ultimately supersede the NUREG-0700 guidelines.

In Germany, the main aspect of advanced systems to which maximum consideration has been given is related to the hardware and software reliability. As an example the licensing procedures of the DAM stressed redundancy, separation, fail safe, self test, self checking for failure etc. while the main computer software was verified step by step. Moreover in order to avoid that human factors problems can affect the system proper operation, it is impossible by design for control room operator to actuate the system.

It has been noted that in Germany a general set of criteria, graded into four "quality classes", according to the safety significance of the specific system involved (i.e. the maximum amount of radioactive release resulting from a failure of the system itself), are presently under finalization to clearly establish the licensing requirements of advanced I&C.

All these requirements are founded on the following basic criteria:

1) Advanced I&C systems must exhibit the same level of independence, redundancy and separation of the corresponding safety functions.

2) The overall reliability of each single plant system must not be dominated by the reliability of its I&C; i.e. the reliability of I&C equipment must be better than the reliability of the mechanical components.

As regards the monitoring and supervision systems (e.g. PRISCA system), they are not licensed to be used during incidents and accidents, when data from the conventional part of the control room have priority.

Finally, as regards the human factor aspects of computerized I&C systems, licensing requirements are mentioned only rarely and in most cases only basic nuclear and conventional standards on ergonomics are quoted.

In Finland, the systems performing an essential role for the reliability of the main safety functions are assigned at least to the safety class 3, together with those devices necessary to monitor such functions. This approach has been followed also for the CSF (Critical Safety Functions) monitoring system, though it is not considered a safety system.

In Slovenia, Krsko NPP should perform by itself an MCR design evaluation, in accordance with post-TMI requirements, as by now there are no regulatory requirements in this field.

In Spain, the licensing requirements of the SPDS were based on three main aspects, related to instrumentation, procedures and human factors. From a human factors point of view the licensing process is aimed at checking the design compliance with the established human factors principles, in order to assure that the displayed information are complete, easily perceived and understood by the operators. This implies the evaluation of the design documentation and the use of audits during the different phases of the design and the implementation, verification and validation processes.

In England, the licensing process covers explicitly, in a distinct section of the regulator's Safety Assessment Principles, the human factors field with emphasis on task analysis, MMI, operating procedures, safety management systems. Human factors related issues (e.g. the "30 minute" rule) are also treated in other sections due to their interactions with other engineering design principles. As regards in particular the licensing process for "Sizewell B", a specific "Ergonomics programme" was agreed between the utility and the regulator, leaving to the latter the task of monitoring the execution and assessing the soundness of the technical reports specifically prepared and inserted in the Final Safety Report. Major areas of activity were the task analysis of safety actions, including validation exercises both on an MCR mock-up and a full-scope MCR simulator, and the verification/validation of single parts of the MCR design (display navigability, control and alarm handling etc.)

1.3 Evaluation from a Human Factors Point of View

As discussed in the previous chapter, the evaluation/validation of advanced systems is an important part of the implementation process and is the only effective way to find out and solve errors,

discrepancies, deviations from expected performances, i.e. generally speaking, to assure the complete compliance of the system with the established design requirements.

In Spain the evaluation of the SPDS installed at Asco plant was performed by an independent engineering firm, that took under consideration both ergonomics aspects (operator response time, MMI versatility and auto diagnosis). The review was followed by a validation performed by the Vendor through a computer code specifically adapted to Asco plant, in order to avoid any extrapolation or interpretation of data. Moreover, after the system implementation, the regulator performed an evaluation, confirming so far the complete compliance of the system with all applicable standards.

In Hungary the evaluation of the VERONA system was based on factory and on-site acceptance tests, presently still under way, conducted by a team of computer and reactor physics experts, that in the future will be also responsible for the operation and maintenance of the system. During the site tests the new system is being operated in parallel with the old one in order to facilitate the comparison of the results. Several minor modifications affecting the ergonomic aspects and some software bugs were identified and corrected.

The evaluation of PIS installed in the Slovenian plant of Krsko, still to be made, will essentially follow the guidelines contained in the NUREG 0700. From the first year of experience it is however already clear that a particular effort is to be put in the operator training, especially people without computer familiarity, and in the reliability of field data used by the system.

In Finland, after an in-depth evaluation of the CSF monitoring system, performed by the utility at the Loviisa training simulator, another specific test program was executed, on request of the Finnish Centre for Radiation and Nuclear Safety (STUK), to demonstrate the behaviour of the system in particular during degraded transients and accidents.

The evaluation of SPDS designs for all operating U.S. plants was performed by the NRC on the basis of NUREG-0800, NUREG-0700 and Supplement 1 to NUREG-0737. This activity identified several deficiencies in the initial design and operation of SPDS. For example, the information selected for display at some plants was insufficient to adequately represent the plant safety status. At some other plants, the SPDS gave the operator more information than could be assimilated in a reasonable time. Often, the licensee did not involve their plant operators in the development and testing of the SPDS. This resulted in systems that operators did not accept. The licensees have now corrected these deficiencies, and every operating U.S. plant now has a working SPDS.

The evaluation of the Sizewell B MCR, from a human factor point of view, was an activity that started early in the design phase to consider allocation of functions, task analysis and the proposed MCR staffing level. Typical identified problems were related to insufficient information procedures/displays, discrepancies between displays, procedures and control labels, lack of feedback, difficulties in information processing etc. After that, detailed walk-through exercises were undertaken using a MCR mock-up in order to assess the quality of the operating procedures and their compatibility with the overall MCR design and to confirm the adequacy of staffing arrangements. An interesting outcome of this evaluation phase was that, during the first 30 minutes post-fault, a two-person team could function properly, but could have some period of high workload; there is therefore a benefit in the control room support engineer being available at an early stage after the fault. The navigability of the computerised display system (with approximately 800 separate formats) was investigated under experimental conditions. The final validation of operating procedures and the MMI was undertaken with the full-scope simulator: the full analysis of the results is not yet available.

The Swedish SAS-II system was developed and validated through a joint program between a nuclear power plant, the utility, the vendor, the Halden Reactor Project and the Swedish Nuclear Power Inspectorate, which in particular verified that sufficient knowledge and competence were represented in the development of the system, with emphasis to human factor specialists. Eleven Reactor Operators (ROs) and Senior Reactor Operators (SROs) participated in the validation study, being exposed to four different and independent test scenarios. The aim of the tests were to check whether the system use originated a time reduction in operator responses, a better quality in the supervisor understanding of the scenarios, an improvement in operator problem solving strategy. Although none of the three previous hypotheses were clearly supported by the test results. The results, however, showed the importance of guidance by Emergency Operating Procedure (EOP) to prioritise and focus on key information provided by the system. The system

seemed to comprise more information than needed to handle the disturbance situations. The validation phase highlighted the necessity of some modification to the system as well as further training of the operators.

Chapter 2

Alarm Processing as a Support to Operators

One of the major issues in developing advanced control rooms is the adoption of an improved alarm system that, from one side, solves the problems related to the operator cognitive overload and to the alarm avalanche during fast transients or accidents and, from the other, provides adequate support to the operator in relation to his enhanced supervisory tasks, typical of advanced control rooms.

In Spain, the Alarm Logic System installed in Almaraz plant represents an attempt to deal with the problems of organising the alarms in functional groups, applying filtering criteria, using priority codes, cut-out conditions, variable limits.

Human factors have been widely considered in developing the Alarm Logic System. In particular the following main concepts have been applied:

1. Use of temporary operator defined alarms or alarm-set points;
2. Intelligent alarm conditioning to prevent unnecessary alarm occurrences;
3. Avoidance of multiple-input alarms;
4. Alarm number reduction, using filtering and conditioning logics, providing however to the operator the capability to access the suppressed alarm information.
5. Alarm prioritization using a reduced number of high priority alarms such that the need of display paging is avoided;
6. Alarm sequence recording with a millisecond time resolution. The sequences are stored in large files containing 10 000 events. Retrieving capability is supplied to the operators.

A detailed verification process has been performed in two time phases to check system compliance with man-machine interface requirements. This process has been executed by highlighting the system completeness and consistency and giving special emphasis to the characteristics of the alarm system design related to the area of Human Factor Engineering. Although it is recognised that the most effective validation method is conducting real-time dynamic simulation, a static validation method for revising the system software and the implementation of the logics was used, due to the fact that the validation process was performed before the system start-up at the site. This process included the verification of the operator understanding of the supplied information and of an efficient communication between the operator and the system.

In Slovenia an evaluation of the existing alarm system has been performed in two steps: firstly an analysis was carried out, based on NUREG-0737, to identify unnecessary alarms causing operator overburden. The following step was that of eliminating those alarms, that appear after the operator has turned off some active components and therefore do not give the operator any additional valuable information.

A PWR Advanced Alarm System of incidents and accidents was developed in Japan to reduce the potential of human errors. This system was incorporated into the main control panel of the Kansai Electric Power Co., OHI nuclear power plant units 2 and 4.

The new alarm system has been designed to enable the operators to identify the most important information and grasp the real plant status by using colour-coded LEDs for alarm windows that dynamically change their colour depending on the importance or priority of the alerting information, as follows:

- RED: Alarm Information, requiring immediate action;
- YELLOW: Alert Information, requiring a check for proper operation of automatic systems;
- GREEN: Normal Information.

The PWR Advanced Alarm System was developed in the following steps, leading to a full-scale prototype production and connection to a simulator to perform comprehensive verification tests:

1. Identification of problems related to conventional alarm systems;
2. Survey of design improvement in the world;
3. Analysis focused on causal relation of alarm;
4. Study of alarm display patterns, on the basis of a selection of 120 main alarms;
5. Study of dynamic alarm colour coding rules;
6. Fabrication of miniature alarm model (120 main alarms); and
7. Test of the system from the operability point of view.

Chapter 3

Expert Systems

In Hungary a three year project has been started in late 1991 in the field of computerised operator support systems using expert systems. The main targets of this project were the development of a Personal Computer (PC) based, task oriented "information an expert system" and the implementation of an add-on computer sub-system, built in the framework of a real time expert system shell.

The scope of the project is to produce a pilot version of an expert system based on the latest software technology, capable, in terms of speed and flexibility, to be applied to process monitoring and to enhance operator understanding of the plant status in whatever situation.

The PC based "information and expert system" (first target of the project), based on MS Windows environment running on 486 PC, is structured in a modular way as follows:

1. Cause/consequence analysis module supplies information on the primary causes (and consequences) of a disturbance in the plant.

2. Early fault detection module monitors and analyses signals from the plant components.

3. Fluctuation diagnosis module performs spectral analysis algorithms on the measured time series.

Each of these modules is, in turn, constituted by several simpler software sub-modules performing low level evaluations.

The second target of the project a compute based sub-system prototype of an on-line, distributed, information system for VVER-440 plants. This system integrates and combines information received from the following computerised operator support systems (COSS) and expert systems:

- plant computer,
- core-monitoring system,
- automatic disturbance analysis expert system using fault tree analysis,
- neutron, thermal and pressure fluctuation diagnostic system for early fault detection and noise analysis.

At the present, pilot stage system will be used mainly by plant engineers and reactor physics experts. At a more mature stage the system could be placed in control room to enhance operator monitoring and understanding.

An 8-years (1984-1991) project, called Man-Machine System for Nuclear Power Plants (MMS-NPP) was developed in Japan under the sponsorship of the Ministry of International Trade and Industry and the participation of several private companies.

The aim of the project was the realisation of an advanced operator support system through the application of new technologies such as computer and artificial intelligence techniques, in order to support a good understanding of imminent plant conditions and a best inference and judgement matching the operator's cognitive processes in the decision making of operational strategies.

Four functions were provided by the MMS-NPP:

1. Normal operation support function as operator aid in performing start-up, shut-down and load following.

2. Anomaly and accident management support function, by identifying plant status and possible causes of plant anomaly, predicting the potential plant status changes and offering adequate operator guidance for corrective actions.

3. Maintenance work planning support function to check any possible adverse influence of the maintenance activities on plant performances and to optimise system and component isolation for best plant operation.

4. Optimal operation monitoring function (intelligent MMI) to provide the operator with various information to facilitate the process of operator's decision making.

A verification process of the MMS-NPP was performed to check the compliance with the design targets, in particular the reduction of work load, the improvement of operational reliability and the enhancement of operational quality.

This analysis performed by incorporating the system into Boiling and Pressurized Water Reactors (BWR and PWR) simulators has given favourable results that can be resumed as follows: a substantial reduction has been obtained of both physical and mental work loads and a significant enhancement of operational quality has been obtained by a quicker and uniform detection of event occurrence and termination.

Chapter 4

Task Allocation Between Man and Machine

The proper balance between automation and human actions in nuclear power plant design is certainly one of the major issues, as it heavily affects both safety and reliability of plant operation. Some general principles should be followed when assessing the opportunity to assign a specific task to man or to machine, remembering that each of them has some peculiar features that makes it more suitable than the other to a given task.

For example, automation should be used to protect society from the fallibility and variability of humans and therefore should be used in high risk areas, or when a large quantity of data are to be treated or when high accuracy, repeatability or rapid performances are required. Humans, on the contrary, should be chosen for tasks requiring inferential knowledge or a peculiar flexibility or when an excessive cost is connected to the automatization of the task. In any case, once a task has been allocated to the machine, it is not generally appropriate to ask the operator to act as a back-up in cause of machine failure: to assign new sudden tasks to an unsuspecting operator is a prime example of poor design.

Use of a well-balanced allocation process will optimise the contribution of both man and machine to the overall system performance; nevertheless different solutions ar possible to the same problem depending on the different inputs, specific circumstances and required safety targets. This determines, as an outcome, significantly different automatization level, especially when future plant designs are considered.

The NRC has developed in the United States, new guidance for advanced MMI technology us. This guidance is provided in draft NUREG/CR-5908 containing an eight-element Human Factors Engineering (HFE) Program Review Model. Element 4 provides criteria on man-machine task allocation.

The NRC expects that the advanced plant designers will avoid allocating functions that would be impacted by human limitations and that the design process would be conducted according to accepted HFE principles using a structured and well-documented methodology.

The design acceptance criteria of NUREG/CR-5908, contained in Element 4, include:

- all aspects of system functions definition must be analysed in terms of resulting human performance requirements;
- sensitivity, precision, tie and safety requirements, in addition to the required reliability of system performance, must be considered when allocating a function to operator or to a system;
- trade-off analysis must be performed to determine adequate function allocation where alternative concepts are considered.

Guidance documents cited by the NRC are NUREG/CR-2623, NUREG/CR-3331 and IEC 964.

In Italy, in the framework of the study of the next generation passive plants, a new concept of the operator role has been developed by ENEL, taking profit of the main feature of these plants i.e. the use of passive systems for the safety function implementation. In this context no credit is given to any operator action, during the first 24-72 hours after any initiating events (grace period), in evaluating the compliance with the external release regulatory limits. In fact, in case of a licensing basis event, the reactor, after being

automatically shut-down, is cooled by passive safety systems and in case of beyond licensing events, even if core damage occurs, external release regulatory limit shall be met without the need of operator action during the same grace period, thanks in particular to a significant increase of containment design performances.

Introducing these concepts, the operator should no more be considered a "fast actuator" but an "intelligent supervisor", monitoring and supervising plant functions during normal operation and transients in order to make unnecessary, if possible, the intervention of the passive safety systems, to optimise plant operation avoiding unnecessary loss of plant availability and protecting the investment avoiding events leading to possible fuel and component damage.

This new role is obtained by using passive safety systems, digital technology for the MMI and adopting a high degree of plant automation. All these aspects lead to the definition of a completely new allocation of functions between man and machine.

In Norway, at the Halden Reactor Project, a specific project is under development called Classification of Operator Support Systems (COSS) with the aim of assisting the operator in nearly all operational situations met in the control room. Three different plant statuses have been defined:

1. During normal operation it could provide useful functions such as an efficient control of power distribution in the reactor core for improving plant efficiency (example of the general function of status identification), faster than real time core simulation to develop short term control strategies (example of action planning), control sequence computerisation (example of action implementation).

2. During disturbances, the same general function could be considered in assisting the operator to identify the plant status, to plan the action to be performed and to operate the systems involved in the disturbance. Several tools are available or are under development world-wide in this field.

3. Finally during accident situations, computerised operator support systems have had a large diffusion in NPPs in order to facilitate operator handling of such situations. Safety Panel Display Systems help the operators to detect when a safety function has been triggered. An extension of the detection principle is the need of alarming the operator before the triggering limit is reached, by using trend diagrams for the critical function parameters. On the base of these principles, a limited prototype of Integrated Surveillance and Control System (ISACS) has been developed at Halden laboratories. It will be integrated in the PWR simulator in Halden Man-Machine Laboratories (HAMMLAB).

Many COSSs have been developed and verified at Halden, running realistic scenarios on a full-scale simulator. As a result, improved operator performances have been obtained. Studies in this field are continuing at Halden.

Chapter 5

Methodologies for MMI Human Factor Evaluation/Validation

In France the S3C control room assessment was jointly performed both as regards the technical and the ergonomic aspects to verify that the operator interface allows him to operate without restrictions and in a very efficient manner under the best possible conditions.

The ergonomic part of the assessment was performed subdividing S3C design in many different subjects or topics (alarm dialogue, station design, physical control resources, computer interfaces, information processing by operators, collective work including job sharing and communication, etc.).

The method used for the assessment was based on several ergonomic specialists observing the operators at work on the simulator during normal operating conditions, cold shut-down, main transients and certain incident and accident situations.

The results of these tests were firstly integrated with direct interviews to the operators and then filed in a computer system for subsequent analysis. The results of the analysis were therefore compared with the hypotheses to be verified.

The application of this methodology provided significant benefits in the ergonomic assessment of the N4 series control room and instructive suggestions for future improvements. In particular dealing with real statistically analyzed data was a major positive aspect, while the fairly empirical manner to judge the effectiveness of the plant control and the fact that only safety aspects were subjected to official comments were certainly points needing an improvement.

Finally, as the impossibility of guaranteeing a sufficient reliability of computer hardware and software required the addition of an auxiliary conventional panel, significant problems can potentially come out, essentially linked to the necessity of controlling the plant through an interface different from the normal one and to the sudden loss of all the computerized aid (in particular alarm processing) normally available at the workstations. The next assessment stage in the framework of the S3C project will in fact consist in ensuring that the use of the auxiliary panel does enable all the situations to be controlled by the operators.

In the United States, for the evaluation of human factors aspects, NRC uses the criteria provided by NUREG-0700. However, since this document gives only limited guidelines for reviewing advanced digital applications, NRC is developing new and more applicable guidelines. The draft NUREG/CR-5908 contains criteria for the following eight elements of Human Factor Evaluation (HFE):

1. human factors engineering program management
2. operating experience review
3. system functional requirements analysis
4. allocation of functions
5. task analysis
6. human-system interface design
7. plant and emergency operating procedure development
8. human factors verification and validation.

The new guidelines will be used by the NRC to evaluate proposed MMI designs for the advanced plant designs with the aim to verify that human factors principles have been properly incorporated and to provide assurance that the plant staff can use the design satisfactorily in a manner that limits operator errors.

The Halden Project performed some evaluation studies using the HAMMLAB which consists of an experimental control room coupled with a full scope simulator based on the PWR plant of Loviisa VVER in Finland.

The test evaluation performed in several experiments have clearly demonstrated that HAMMLAB has several features that yield it useful to the investigation of man-machine interactions, showing also that, after a short period of adaptation of the operator with the unusual experimental control room, the artificial situation places few constraints on their work.

Human factor evaluations of the hybrid control rooms of the newest reactors in Sweden were performed after a request by the Safety Inspectorate. Before operation, evaluations were made by human factor specialists and operators with the help of guidelines, and talk-and-walkthroughs. Further evaluation during operation was requested and an evaluation method was developed addressing operational experience. Operators were interviewed regarding task demands, the human-machine interface, plant information system, training and organisational resources for handling the demands. They also assessed processes for organisational learning from encouragement of problem identification to implementation and evaluation of changes. Based upon the interviews, a questionnaire was developed and distributed to all operators. The results were fed back to the crews and the plant management. The actions taken by the plant in response to the results were also used as an input to the assessment of the improvement capacity of the organisation.