Human factors in the operation of nuclear power plants

Improving the way man and machines work together

by E. Swaton, V. Neboyan, and L. Lederman

In large and complex interactive systems, human error can contribute substantially to system failures. At nuclear power plants, operational experience demonstrates that human error accounts for a considerable proportion of safety-related incidents. However, experience also shows that human intervention can be very effective if there is a thorough understanding of the situation in the plant. Thus, an efficient interface of man and machine is important not only to prevent human errors but also to assist the operator in coping with unforeseen events.

Human reliability can be understood as a qualitative as well as a quantitative term. Qualitatively it can be described as the aim for successful human performance of activities necessary for system reliability and availability. Quantitatively, it refers to data on failure rates or error probabilities that can be used, for example, for probabilistic safety assessments (PSAs).

Education and training

Qualified personnel are central to ensuring safe and reliable operation of a nuclear power plant. Their continuing education is necessary so that required performance levels are achieved and maintained; it includes initial training, retraining, and the updating and broadening of knowledge and skills. While each country has certainly developed its own educational system depending on national conditions, the particular skills required of nuclear power plant personnel anywhere are common, since there can be no compromise for the safe and reliable operation of a nuclear power plant. Thus, each country's nuclear power training programme has to attain the same level.

One primary skill, particularly in the future, will be adaptability, that is, the ability to cope with unforeseen circumstances. It means being able to find, to recognize, and to formulate a problem — and deciding if the problem ought to be solved, as well as how to solve it.

While education refers mainly to formal studies and continued competence, training is oriented towards job-specific tasks. Apart from training performed in classrooms or on the job, the utilization of simulators for this purpose has attracted particular attention. Most countries with nuclear power plants have simulator training programmes, generally well developed. But their value can be limited by the simulator's age, type, size, and capability. However, simulator training and retraining is indispensable for improving safe plant operation and providing the knowledge and skills for plant control under normal and abnormal conditions. Furthermore, benefits of simulator training can be seen for two aspects. One refers to PSAs, where the insights gained can be used to select scenarios for training. Simulation experiences also can be used to update and improve PSAs. The other aspect relates to the possibility of evaluating plant modifications from the standpoint of human factors. This includes new equipment, the correctness and practicability of normal and emergency operating procedures, and the adjustment and updating of training programmes.

Simulator training

In use for many years as a major tool for nuclear power plant operator training, full-scope simulators have become very sophisticated instruments. We can now treat training scenarios that couldn't be treated 5 years ago. What will we do with the computing power we will have in 5 years? On the one hand there are specialists who feel that more computing power is necessary to provide more extensive training. The overall feeling, however, is that the computing power now available is adequate to do the job. At the same time there is an evident move to increased fidelity models. Over the past 5 years, much emphasis has been placed on high fidelity of simulation for the reactor core model and the reactor coolant system model. Whether increased fidelity is justified requires more thought and consideration. It is one thing to provide higher fidelity, and it is another, more important, thing to determine the need for it because existing models cannot meet training objectives. A recent IAEA specialists' meeting on training simulators for nuclear power plants showed that some designers identified training requirements that motivated model development. This is a good sign. The design of training simulators should be guided by the examination of learning objectives. This has not been the case in the past.

Ms Swaton, Mr Lederman, and Mr Neboyan are staff members in the Department of Nuclear Power and Safety.

A full-scope simulator is a powerful tool, but because of its complexity and costs, it is not always suitable to cover all training needs. It has been estimated that 75-80% of total training can be provided by representing only 25-30% of the full-scope simulation control room.

To cover training more devoted to the understanding of a part of a plant or of limited functions, "part-task" simulators are being used. These are either in the form of a plant analyser, a micro-simulation system, or a "function" simulator. In these cases, the formation of an appropriate "mental model" of the system is important. It provides the opportunity to think through the operation to be performed, by concentrating on the ability to process and utilize spatial information. A good illustration is the use of a semi-scale mock-up of a pressurized-water reactor (PWR) coolant system (called glass models). Even though the pressures used are not prototypical, the training value of being able to visualize the thermodynamics directly is very important.

Regarding further developments in the field of training simulators, attention has been drawn to the following problem: the process of the brain, how do we learn and how do we approach the man-machine interface problem with a better understanding of human cognitive skills, so as to reduce operator overloads and enhance performance?

Review of experience with simulator training for emergency conditions showed that safety-significant incidents often present operators with a situation that evolves and develops quite differently from the scenarios on the simulator. In addition, since emergency conditions are rare events, prediction and analysis of human performance presents certain difficulties. However, the overall usefulness and importance of simulator training for severe plant conditions is generally recognized, especially if accident scenarios are designed in such a way that sequences can be started at different power levels and the simulation can proceed until degraded core conditions are reached. Furthermore, if an error is committed by the trainee in handling a particular situation, the simulation can be stopped, and the error can be pointed out and discussed. Subsequently, the scenario can be resumed, thus providing a valuable feedback for both the instructor and the trainee. In a systematic manner, data can be collected by means of automatic systems monitoring trainee performance or the establishment of a scheme that reports errors for the instructor. PSAs are making increasing use of data on human performance collected from simulator sessions.

Human error data collection

Analysis of abnormal events and insights from PSAs have demonstrated that a large proportion of cases have their origin in erroneous human performance. The main source of information on human behaviour/error is the operational experience at nuclear power plants. Apart from the national reporting practices of safety-related events to the regulatory authorities, several international reporting schemes do exist. The Incident Reporting System (IRS) of the Nuclear Energy Agency of the Organization for Economic Co-operation and Development (NEA/OECD) collects typical examples from Western Europe, Canada, Japan, and USA. The IAEA-IRS is basically similar but also includes reports from Eastern European and developing countries. Another system — the Abnormal Occurrences Reporting System of the Joint Research Centre in Ispra — collects information contained in some national systems. However, human errors are not specifically identified in these reporting schemes, and analysis methods have to be developed to single out the human performance contribution to the accident. Only in a few cases have utilities started systems dedicated to identifying the role of human errors in incidents.

Several general situations have been identified:

- Activities such as testing and maintenance are a common cause of errors. Implementation of automatic procedures may alleviate some problems.
- Human errors are more frequent in systems having low levels of availability or redundancy, or those not sufficiently automated.
- Human errors in abnormal conditions are more frequent just after alarms have been initiated.
- Bad design (from viewpoint of system engineering, control-room layout, and ergonomic principles) is a major cause of human error.
- The transfer of information during shift changes of personnel is a general cause of error.

PSAs provide valuable insights for determining the plant systems which are subject to human interaction and for aggregating these interactions in terms of similar tasks or common causes. However, the general lack of real data on human behaviour, especially under abnormal conditions, imposes limits. In this area, PSAs should only be considered as indicators of potential human problems and not as predictors of human behaviour.

Information feedback

Accident analysis provides the possibility of understanding human errors to some extent. An operator has to get feedback, but the question is how to establish specifications for assessing it.

In solving problems related to human error and the implications of operational experience, some countries seem to focus on databases, others on simulators. In this situation the question can be asked: How should we capture operator experience, and how can one judge various benefits of different aspects? Should designers have a strong strategy? Research has to continue in this area, in different directions, and co-ordination seems to be necessary, in the view of many experts.*

* This was the common opinion of experts at the IAEA's specialists' meeting in Roskilde in May 1987 on "The human factor information feedback in nuclear power: Implications of operating experience on systems analysis and operation".

Feedback on the role of human factors in significant events is being analysed nowadays in several research centres. The US Nuclear Regulatory Commission (NRC) has established a formal Incident Investigation Program (IPP). One objective is to assure that operational events are investigated in a systematically and technically sound way. Every scram has to be reported to the NRC, and the purpose of the IPP is to depict the situation realistically.

In Japan, an incident report for a databank has to be made within 48 hours, and a full report within 30 days. The rate of human error for the total number of incidents is approximately 10%. More than half (54%) of the cases resulted in automatic shutdown; 15% in plant power reduction; and 31% had no effect. Half (51%) of the causes of human errors were due to insufficient maintenance, and 29% were due to improper operation.

One estimation, by a Belgian expert, showed that out of 40 scrams for seven reactors, 70% had a human related factor. An in-depth statistical analysis performed by Electricité de France (EdF) showed relatively few errors during the night when there is little activity, and during the lunch hours. The most common types of errors included omissions and delayed operations. As for mechanisms of errors, the most common are forgetting to perform an operation and the failure to identify the correct operation, together with a bad diagnosis of the state of the system.

Simulation can also deliver efficient feedback for operator behaviour, but effective research will demand a great deal of money and effort. In order to get rapid feedback from operator experience, for example, a full-scope simulator of a computerized control room was built in France.

Operator support systems

Operator support systems refer to a class of devices designed to be added to a nuclear power plant control room to assist the operator in performing his job and thereby decrease the probability of human error. They encompass a wide range of devices from the simple, such as colour coding a display to distinguish it from a group of similar displays, to the complex, such as a computer-generated video display that concentrates a number of scattered indicator readings located around a control room into a concise display in front of the operator. Major efforts have been devoted to the development of computerized operator information and support systems.

Depending on the pre-defined purpose, different systems have been conceptualized. While early systems were primarily devoted to monitoring critical safety functions and the detection and location of disturbances, later systems surpassed this limited scope by additionally providing information on the normal plant configuration as a function of the mode of operation and predictive plant behaviour.

This increasing reliance on computerized operator support systems should be examined in the light of tasks to be performed, thus emphasizing the relative strengths of humans and computers.

Identification. While computers are good at recognizing pre-defined patterns, humans are superior in recognizing any pattern which might evolve. Humans are furthermore able to handle incomplete information. The strength of computers lies in measurement sensing and validation, and in handling complex computations. For identification, they predominantly rely on deductive processes based on given rules.

Analysis and interpretation. Complex algorithmic operations can be handled by computers in a very fast and reliable manner, but computers have limited capacity for application of heuristic operations. In contrast, humans can generalize across samples, using judgement, experience, and implicit knowledge.

Comparisons. Processing and recollection of large amounts of precise data, and comparing them based on pre-defined rules, is clearly a strength of the computer. However, humans are able to make use of data from various sources and in different formats for their comparisons, drawing more on experience than on precise deductions.

Planning. Given the task of finding an optimal solution in a well-defined problem, computational power is certainly an advantage. Slight alteration of the problem brings out the strength of the human, who can quickly adapt existing procedures to suit the situation and can even design new procedures if so required.

In general, computers can only function efficiently and reliably if they are dealing with problems, knowledge, and rules or procedures that are very well defined. Human operators can perform under these same conditions but can also handle ill-defined problems, incomplete knowledge, and insufficient rules or regulations. Thus, humans are still able to control the system in situations where the computer is bound to fail. Consequently the fact that computers can perform some tasks better should not be cause to replace the human operator.

PSA information for safety decisions

Over the past 15 years, PSA has become a prime tool for evaluating reactor safety. More than 30 PSAs have been completed and the results have brought invaluable insights for plant design and operation. Despite its potential, the actual use of such studies in decision-making has been very modest. One reason is that PSA reports mix useful results with a great deal of technical information that is irrelevant to decision-makers. Another reason is that PSA reports are understood only by those who are well versed in the methodology.

Some years ago work started to allow for a more immediate and interactive use of the information contained in a PSA. The objective of these efforts was to

create a "living PSA model", readily available for operational safety management.

During the same period small computers, especially personal computers, developed in a remarkable way. Therefore, small computers as stand-alone facilities or as work stations linked to larger computers are used today in many branches of industry.

Likewise, the integrated systems which have been developed to structure PSA information make use of recent developments in the technology of small computers. Due to their highly interactive and "user friendly" characteristics, these systems are particularly suitable for updating PSA information and for responding to "what if" questions.

Applications of PSA information for operational safety management are based on the effect that changes in plant configuration may have on overall plant safety. They include control and assessment of the status of the essential safety systems; modifications in operational procedures; changes in technical specifications (in particular those regarding test and maintenance and allowable outage times); prioritization of items for repair; evaluation of design changes considering the interactions between plant systems; prioritization of inspection activities.

Current developments are aimed at providing information for decision-making under normal plant operation conditions. Software packages include a model of the plant based on results from fault-tree and event-tree analyses. Utility personnel and regulators are the main users of these software packages.

Two recently developed systems are:

PRISIM (Probabilistic Safety Information Management System). This is a software package for personal computers that permits rapid access to PSA-related information. The database contains both pre-processed information obtained from the baseline PSA results and a plant safety model that allows assessment of changes in plant safety caused by changes in plant conditions. Safety issues involving changes in plant configuration can be handled by a model that allows the user to specify (based on schematics or component lists) a new plant status and to calculate the resulting safety margin. Various measures of importance are introduced to rank safety systems and operator actions. The code can also investigate the response of safety systems to particular failures. This investigation can uncover design weaknesses, such as vulnerability to support system failures. Pre-processed information from baseline results of the PSA includes a description of the most important accident sequences; operator recovery actions; support system interfaces; a library of technical specifications; and priority rankings for safety-related systems, subsystems, components, and operator actions. PRISIM was developed for the US NRC to assist inspectors. It is presently installed at several nuclear plants, namely Arkansas Nuclear One (Unit-1), Peach Bottom-2, and Surry-1.

ESSM (Essential Systems Status Monitor). The ESSM is a software system, based on fault-tree analysis techniques, which provides on-line facilities to plant operators. It enables them to quickly perform certain probabilistic assessments of plant systems in an interactive environment. Keyboards and visual display monitors in the central control room are used to enter and display the current status and configuration of plant items. At any time the operators may request ESSM to assess the overall availability of the essential systems. ESSM will analyse the complex system fault trees (which model redundancy and complex system interactions) taking into account the effect of current plant outages and configurations. It then displays to the operator the availability status of the essential systems that has been determined using probabilistic criteria. At the same time, ESSM monitors deterministic operating rules. If rule violations demand remedial action, then all relevant information is displayed to the operator. In addition to its assessment facilities, ESSM provides the operator with recommendations for urgent maintenance and provides a maintenance planning facility. ESSM has been recently installed in the United Kingdom at the Heysham-II nuclear plant.

International co-operation

Many possibilities exist to strengthen the human factor in nuclear power plant operation. This can be achieved by engineering measures to improve equipment or by measures to improve operator behaviour. However, there seems to be no general agreement as to which measures to take and where to place priorities. This was one reason why the IAEA convened the International Conference on Man-Machine Interface in the Nuclear Industry (Control and Instrumentation, Robotics and Artificial Intelligence).* Hosted by the Government of Japan in Tokyo, from 15-19 February 1988, the conference was organized in co-operation with the NEA/OECD and the Commission of the European Communities (CEC). Topics included analyses of human behaviour in plant operation, reviews of human engineering measures to improve human performance, and the importance of providing the operator with more and better information.

* Proceedings will be published by the IAEA.