INTEGRATION OF ERROR TOLERANT CONCEPT INTO THE DESIGN OF CONTROL ROOM OF NUCLEAR POWER PLANTS

K. Sepanloo[1], N. Meshkati[2], M.A. Azadeh[3], F. Moatar[3]

[1] Nuclear Safety Department, Atomic Energy Organization of Iran, Tehran, Iran
[2] Institute of Safety and Systems Management, University of Southern California, Los Angeles, USA
[3] Department of Physics and Nuclear Technology, Amir-Kabir University of Technology, Tehran, Iran

RU9604415

INTRODUCTION

Human error has been recognized as the main cause of accidents in complex technological systems. This has caused increasing concern with the human involvement in technical systems safety. Data on human reliability in control rooms indicate that human reliability is unacceptably low (Hollnagel 1988). This is particularly important under difficult unexpected situations where the operator's deteriorated performance may lead to irreversible hazardous processes in the plant. It is generally recognized that the most important functions exercised by operators are those of decision making at critical junctures during the course of an accident.

The present complex, large-scale technological systems pose additional demands on the human operators. These systems require operators to constantly adapt to new and unforeseen system and environmental demands. Furthermore, there is no clear-cut distinction between system design and operation, since the operator will have to match system properties to the changing demands and operational conditions. In other terms, according to Reason (1990), operators must be able to handle the "non-design" emergencies, because the system designers could not foresee all possible scenarios of failures and are not able to provide automatic safety devices and/or remedial procedures for every contingency. Therefore, it is highly important that the operator's job, which involves effortful and error-prone activities of solving and decision making at the workstation level, be facilitated by proper interface devices and be supported by the needed organizational structures.

THE IRONIES OF AUTOMATION

Modern microprocessor technology and knowledge-based decision systems have made it entirely feasible to automate much of the nuclear power plants control room functions previously performed manually. There are many real benefits to be derived from automation; the question today is not whether a function can be automated, but whether it *should* be, due to the variety of human factors questions which are raised. It is highly questionable whether total system safety is always enhanced by allocating functions to automatic devices rather than human operators and there is some reason to believe that control room automation may have already passed its optimum. There is usually an image of automation as quiet, unerring, efficient, totally dependable machines, the servant of man, eliminating all human errors. However, there are many evident related to the operation of automated systems that reject this idea of having absolute trust in automation. For example, it has been found that there is, on the average, three errors in one thousand lines of computer programming (Carnino 1990). There are also ample instances of adverse impact of automation on flight-deck performance. In aviation industry, auto-pilot idea has already been rejected due to: 1) frequent failure of automatic equipment; 2) automation induced errors; and 3) loss of proficiency by the pilot. It is worth noting that the general public appears as sceptical of the infallibility of automation as they are fearful of its consequences (Wiener et al 1982).

For the foreseeable future, despite increasing levels of computerization and automation, human operators will remain in charge of the day-to-day controlling and monitoring of complex technological systems. Operators are kept in these systems because they are flexible, can learn and adapt to the peculiarities of the system, and because they are expected to "plug the holes in the designers' imagination" (Rasmussen 1980). Based on analyses of real emergency cases in nuclear power plants, it has been found that due to tightly-coupled, complex, highly-interactive nature of the system each incident has its own singular character and therefore there is little point in trying to create a predetermined set of typical operator automatic responses to an emergency (Reason 1988). The automatic safety systems are believed to be suitable for coping with "designer-expected"

incidents and the efforts to curb the threat posed by stressed operators by automatic safety systems does nothing to limit a far more likely danger: that they have already been "sabotaged" by maintenance and testing errors (Reason 1987). The adverse impact of committed human errors in other parts, such as maintenance, on the availability of automatic systems and safety of nuclear power plants has also been identified by Meshkati (1991).

THE FALLACY OF THE DEFENCE-IN-DEPTH

Defence-in-depth has been accepted widely as a safety philosophy in which the retention of hazardous material is maintained by putting overlapping layers supported by active safety systems. More over, the integrity of the layers is ensured by putting margins into the layers and systems. The opacity of the safety layers and indulging feature of them towards the impacts of human errors allow the errors to remain hidden inside the system quite a long time. Thus, besides the undeniable safety advantages, this strategy makes the system somewhat ignorant or forgiving towards the occurrence of hardware faults or human errors. The latent errors may also be put in the system in a number of other ways such as design deficiencies, bad management decisions, maintenance errors and poor operating procedures. The more complex and opaque the system, the greater will be their number. For the most part they are tolerated, detected and corrected, but in some cases, a set of "local triggers" combine with these "resident pathogens" in subtle and often unlikely ways to thwart the system's defence (Reason 1988, 1990).

ERROR TOLERANT SYSTEMS

Human error, is considered to occur if the effect of human behaviour exceeds a limit of acceptability. Of course, it is necessary to distinguish clearly between the types of errors induced by inappropriate limits of acceptability, i.e. by the design of the work situation and errors caused by inappropriate human behaviour. Furthermore, in many instances, the working environment can also aggravate the situation. In such unfriendly work environment, once the error is committed, it is not possible for the operator to correct the effects of it before they lead to unacceptable consequences, because the effects of the errors are neither observable nor reversible (Meshkati 1994b).

Recently, based on extensive research on the role of human element in technological systems, it is known that human error, as the unavoidable side effect of the exploration of degrees of freedom in unknown situations, can not totally be eliminated in modern, flexible, or changing environments. In order to allow for, and cope with human errors in large technological systems such as nuclear power plants, human errors should be considered as unsuccessful or unacceptable experiments in an unfriendly environment. Therefore, the design of friendly, i.e. *error tolerant* systems (Rasmussen 1988, 1990, 1993, Rasmussen et al 1994; Meshkati 1994) with integrated task and organizational structures should be considered. The interface design should aim at making the boundaries of acceptable performance visible to the operators while the effects of committed errors are observable and reversible. To assist the operators in coping with unforeseen (beyond-procedural) situations, the interface design should provide them with tools (opportunities) to make experiments and test hypotheses without having to carry them directly on potentially irreversible processes.

It is known that in traditional work organizations, various task groups must respond to rapid changes which cannot be thoroughly analyzed before implementation of corrective actions. Also, discretionary decisions are made by different people that often interact to produce an unpredictable outcome. Error tolerance is important here, because incompatibility between the solutions chosen by the different groups can have drastic economic and environmental impacts. One solution is an integrated information system that ensures effective horizontal communication that makes the effects of decisions made by team members visible within the work context of each of the other teams. That is, it should be made clearly visible (and hopefully reversible) when decisions made by one group violates the boundary of acceptable design as specified by the other groups.

To achieve the mentioned objectives the error tolerant concept can be integrated into the nuclear power plants, e.g. into the interface systems in the control room. In this way, the role allocation within groups interacting during the operation should be analyzed to identify the persons whose decisions can have impact on the successful function of the specified control component. The typical decision situations and the action alternatives available to the operators (in case of occurrence of an emergency situation) and the performance criteria guiding them should be identified. The recognition of communication network among the decision makers involved in response to the emergency case is also important. The boundary conditions of safe operation in the

emergency case should be specified to ensure the observability and reversibility of the violations. In addition, it is necessary to specify the indicators to be used for prompting the decision makers to consider the possible violation of such boundaries.

An error tolerant system in the control room of a nuclear power plant has the characteristics of both human-machine and human-human interfaces. It can be regarded a human-machine interface since the operator interacts with the plant through it, and at the same time it is a human-human interface system which informs the other relevant decision makers of the actions taken and also can find the impact of the others' actions on the domain of acceptable behaviour of the operator. Error tolerant system can also be considered as a decision support system, since it provides the operator with the actual state of the plant and the consequences of execution of his commands on the plant. The trend of change of area of the space of possibilities (the degrees of freedom) provides him with valuable guidance in directing the plant away from the safety margin borders. The error tolerant system has the features of *simplicity*, *transparency*, *error detectability*, and *recoverability*. The system facilitates the operator's correct conception about the real status of the plant and enhances the visibility of human actions in the plant both for the operator himself and the others who monitor his actions. Thus, the decisions made and actions taken by any actor are observed and evaluated by a group *mind*, which greatly increases the chance of detection of occurrence of any error. The speed of function of error tolerant system must be faster than the rate of deterioration of the plant state, subsequent to some erroneous executed command. The time needed for the error tolerant system to reveal the incorrectness of the operator's action should not permit the plant to go through irreversible degradation processes. In other words, the error tolerant system should not expose the plant to any danger of inactiveness from the operator to the rapid dynamics of the safety relevant processes in the plant. It is usually the case, since the time constants of most of the changes (e.g. thermal-hydraulics variations) in nuclear power plants are comparatively quite large.

CONCLUSION

Dynamic adaptation to the immediate work environments, both of the individual performance and allocation between individuals, can be combined with a very high reliability only if the errors can be observable and reversible. Error tolerant systems concept is an approach which provides a forgiving cognition environment for the operators to cope with the unforeseen incidents.

REFERENCES

Carnino, A. (1990) *Man and risks*. Marcel Decker publisher, New York, 1990.

Hollnagel, E. (1988) *Plan Recognition in Modelling of Users*. Reliability Engineering and System Safety 22 129-136

Meshkati, N. (1991) *Integration of workstations, job and team structure design in complex human-machine systems: A framework*. International Journal of Industrial Ergonomics, 7, 111-122.

Meshkati, N. (1994a) *A method for managing the integration of error tolerant design in manufacturing systems*. In edition.

Meshkati, N. (1994b) *A method for development and integration of error tolerant design, balancing reliability and complexity*. In edition.

Rasmussen, J. (1980) *What can be learned from human error reports?* In K.D. Duncan, M.M. Gruneberg & D. Walls(Eds), changes in working life, New York: John Wiley & Sons, 97-113.

Rasmussen, J. (1988) *Human Error Mechanisms in Complex Work Environments*. Reliability Engineering and System Safety 22 155-167.

Rasmussen, J. (1990a) *The role of error in organizing behaviour*. Ergonomics, Vol.33, Nos. 10/11, 1185-1199

Rasmussen, J. (1990b) *Human error and the problem of causality in analysis of accidents*. Phil. Trans. R. Soc. London. B 327, 449-462.

Rasmussen, J. (1993) *Risk management, adaptation, and design for safety*. Future risk and risk management. Dordrecht: Kluwer.

Rasmussen, J., Pejtersen, A., Goodstein, L. (1994) *Cognitive Systems Engineering*. John Wiley & Sons.

Reason, J. (1987) *The human contribution to nuclear power plant emergencies*. Conference on human reliability in nuclear power plants 22-23 Oct. 1987. London.

Reason, J. (1988) *Modelling the basic error tendencies of human operators*. Reliability Engineering and system safety 22. 137-153.

Reason, J. (1990) *Human error*. Cambridge University press. England.

Wiener, E., Curry, R. (1982) *Flight-Deck Automation: Promises and problems*. Pilot Error, the human factors, second edition, GRANADA publication, pp 67-86.