Nuclear Society of Slovenia
2nd Regional Meeting: *Nuclear Energy in Central Europe*
Portorož, SLOVENIA, 11.-14.September 1995

THE ORGANIZATIONAL CONTEXT OF ERROR TOLERANT INTERFACE SYSTEMS

K. Sepanloo[1], N. Meshkati[2], M. Kozuh[3]

[1] Nuclear Safety Department, Atomic Energy Organization, Tehran, Iran
[2] Institute of Safety and Systems Management, University of Southern California, Los Angeles, USA
[3] Reactor Engineering Division, Jozef Stefan Institute, Ljubljana, Slovenia

ABSTRACT

Human error has been recognized as the main contributor to the occurrence of incidents in large technological systems such as nuclear power plants. Recent researches have concluded that human errors are unavoidable side effects of exploration of acceptable performance during adaptation to the unknown changes in the environment. To assist the operators in coping with unforseen situations, the innovative error tolerant interface systems have been proposed to provide the operators with opportunities to make hypothetical tests without having to carry them out directly on the plant in potentially irreversible conditions. On the other hand, the degree of success of introduction of any new system into a tightly-coupled complex socio-technological system is known to be a great deal dependent upon the degree of harmony of that system with the organization's framework and attitudes. Error tolerant interface systems with features of simplicity, transparency, error detectability, and recoverability provide a forgiving cognition environment where the effects of errors are observable and recoverable. The nature of these systems are likely to be more consistent with flexible and rather plain organizational structures, in which static and punitive concepts of human error are modified on the favour of dynamic and adaptive approaches. In this paper the features of error tolerant interface systems are explained and their consistent organizational structures are explored.

INTRODUCTION

During the recent years, the researches in human factors have addressed various impacts of organization and management on human behaviour. In the terms of Reason (1990), "we are now in the age of the organizational accident". In many cases human errors are recognized to be the result of mismatch between the human actors and the organization. The organization induced errors offsets the technological modifications if the attitudes and procedures are not changed accordingly. The basis for most existing organizational structures is defined at an early stage in the life period of the plant. During its lifetime many technological changes, and changes to operating patterns and methods inevitably occur in the plant. Organizational structures which were set up for an early mode of operation and which were entirely adequate at that time may not be adequate to properly control the plant after change has taken place.

The term "organization" here refers to relational structure necessary to coordinate the work activities of individuals. A system of cooperative work is an extremely complex organizational phenomenon involving many forms of social interaction. The control requirements of a work domain change over time. A particular division of activities

and, consequently, work groups will evolve for each situation depending on the competencies of the actors, the technology of the work domain, and on the external environment of the organization.

Usually the role of an actor is to control the state of affairs in a work environment that is dynamically changing in response to external conditions and to the activities of other actors. The work organization is then an adaptive, distributed decision and control system interacting with the productive functions and processes. The decision makers and actors are coupled with the work processes through an interface of tools, equipment, and computerized information systems.

ROLE OF HUMAN ACTORS

The basic role of human actors in modern work systems is to act as a flexible analyst and decision maker. The actual state of the system is conceived by the actor on the basis of the information received from the system, including measured parameters as the sources of data, and the mental model that the actor has developed about the mechanisms and features of the plant. The actual state is then usually compared with the nominal target states and the discrepancy is resolved by choosing and implementing an action or set of actions (strategies) among certain alternatives. However, if the effect of an improper decision takes the control function outside its capability limits and thus breaks the closed loop, then proper control is lost, and the ultimate effect of actions including those by other actors (colleagues, supervisors, etc.) depends entirely on the properties of the work system. In that case, a mismatch occurs in the work-actor coupling, an event frequently judged to be a "*human error*" (Rasmussen, Pejtersen, Goodstein 1994).

The mismatch can be the result of change of human actor's behaviour from normal routines or the change of environment in a way that makes the usual human behaviour unacceptable. In both cases, we are faced with a human-system coupling that is too narrowly adapted to the normally successful conditions. Here, the importance of certain interface systems which bridge these gaps becomes clear. The interface must provide adequate flexibility so as to widen the tolerance band when required. This requirement calls for the design of "*error tolerant*" interfaces and their proper organizational context.

HUMAN ERROR

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 environments, 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 1991).

Human errors are intimately connected to adaptation and exploration of the boundaries

of acceptable performance. During this adaptation, performance will be optimized according to the individual's subjective process criteria within the boundaries of his individual resources (Rasmussen 1990a). Unfortunately, perception of the qualities of the work process itself is immediate and unconditional and local adaptation to subjective performance criteria is effective, while the effects on the ultimate result of work of these adaptive trials can be considerably delayed, obscure and frequently conditional with respect to other multiple factors. Short cuts and tricks-of-the-trade will frequently evolve and be very efficient under normal conditions while they will be judged serious human errors in hindsight (Rasmussen 1990b) and under special circumstances they may lead to severe accidents. Disasters such as the Bhopal presents a clear example of how a safe work procedure for chemical manufacturing system, including multiple precautions against human errors, gradually degenerates due to adaptation to locally less efficient work practice (Meshkati 1989 & 1991b).

Purposive human adaptation manifests itself in error mechanisms at all levels of the cognitive control of performance. For problem solving during unusual conditions, an opportunity for test of hypotheses and trial-and-error learning is important for adaptation and for the development of expertise. It is typically expected that qualified personnel such as process operators will and can test their diagnostic hypotheses conceptually, by thought experiments, before actual operation, because the effects of their acts are likely to be irreversible and hazardous. This, however, has the risk of temptation to test a hypothesis on the physical work environment itself in order to avoid the strain and unreliability related to unsupported reasoning in a complex causal net. No explicit stop rule exists to guide the termination of conceptual analysis and the start of action. This means that the definition of error, as seen from the situation of a decision maker, is very arbitrary. Acts that are quite rational and important during the search for information and test of hypothesis may appear to be unacceptable mistakes in hindsight, without access to the details of the situation (Rasmussen 1990b).

COUNTERMEASURES FOR HUMAN ERROR

The major share of human errors in the occurrence of accidents in large socio-technological systems has highlighted the importance of reviewing the current approach towards the concept of human error and design of error proof systems. As mentioned before, when human action transgresses the boundary of acceptable performance we are facing a human error. The boundary is usually defined as preset conditions and relevant procedures which have to be constantly observed. The main goal in pursuit of traditional way of responding to errors is designing less error prone workstations in which the number of human interventions is tried to be reduced to as low as possible.

The current widely used defence-in-depth strategy in large hazardous socio-technological systems, on the other hand, helps the adverse impacts of human errors to remain undetected and be forgiven by the system. The redundant, overlapping safety layers prevent the progression of the chain of individual errors and/or failures from leading to an accident. The large safety margins which are put into the safety layers and systems allow the plant parameters to somewhat exceed the nominal range without serious notification of the operator. The complexity of the control

mechanisms in many cases hinder the operators from obtaining a clear understanding of the real changes in the status of the plant.

Similarly, higher level of automation which is usually deemed as the remedy to human reliability deficiency can not eliminate the problem. The issues such as increase of complexity and opacity of the system specially in unprecedented upset conditions, elevated rate of maintenance errors, loss of skill, de-motivation and passiveness of the operators are some of the adverse impacts of more automation.

Learning from the past experience and subsequent modifications have to a great deal improved the operation of hazardous systems, but it seems that following the current "retro-active" approach of error reduction strategies a certain limit is reached that these strategies lose their effectiveness. As Rasmussen (1993) has pointed out: "attempts to control safety by campaigns seeking to avoid the empirically identified causes and conditions in the future very likely will face 'false alarm' fallacy, in work you simply cannot be so careful as to always avoid all 'resident pathogens' identified empirically in prior cases". This limitation, however, stems from the implicit static definition of error. In the static image of error, there are certain constant specifications and features for the undesired actions which are usually mixed with a shadow of negative terms. Lack of sufficient training, interface deficiencies, stress or more recently, organizational and management faults are only a few of the usually cited "root" causes. Generally, there is an attempt towards the "fixation" of the root causes of errors in response to the revelation of the role of human errors in incidents or accidents.

However, both human being and socio-technological system can not be considered as static items. The personal, cultural, technical, economical and political envelope of the system are constantly changing which require the constant adaptation of human and the organization. Therefore, the concept of error must be viewed in the adaptive dimensions as the mismatch between the two changing sides, i.e. human and system. This non-static mismatch should be bridged by appropriate human-system interfaces which are designed on the basis of dynamic definition of human error.

LEARNING ORGANIZATIONS

Learning organizations are those organizations which dynamically adapt to the changing conditions of the environment. In this process, the boundaries of acceptable performance must continuously and aggressively be explored to optimize the performance. Rather than formulating the rules of conduct, learning organizations use a decentralized closed loop, feedback strategy in which the observed level of safety is compared to a target value and efforts are focused on diminishing discrepancy. In these structures, the safety goals and targets are propagated downward the work system while, in contrast to hierarchial command-and-control management structures, rules of conduct are developed on site and according to the peculiarities of the workplace. The function of higher level management is then not the monitoring of rule adherence, but to supply the needed resources for safety activities and to check work planning methods and performance reports.

For example, in nuclear power plants which are designed according to defence-in-depth principle, the feature of adaptation of different sections to local work requirements may, in some cases, lead to violation of the safe activities of other parts of the plant and provision of a pathway for errors to breach the defence layers and cause accident. Another characteristic of adaptive organizations is that the traditional way of improving safety by increasing the margin to failure is always compensated by adaptive changes. Therefore, the enhancement of safety in learning systems requires adequate knowledge about the mechanisms of local adaptation processes and identification of the important parameters to which the adaptation processes are most sensitive. Also, the safety of adaptive organizations is greatly improved if the actors are provided with appropriate tools to be able to touch the boundaries of acceptable behaviour and can recover from the adverse impacts of their errors, without exposing the plant to undue risks. In other words, adequate flexibility is needed so as to widen the tolerance bands in case of interaction with the limiting boundaries.

ERROR TOLERANT SYSTEMS

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 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 unforseen situation, 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.

An error tolerant system 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. In other words, this interface system provides a means by which the boundaries of safety margins of the plant and the boundaries of allowable actions becomes visible to the operator at any time during the operation of the plant. 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 margins borders. The error tolerant systems have the following features:

- simplicity
- transparency
- error detectability
- linearity
- recoverability

The integration of error tolerant systems into the plant should not add to the complexity of the operation. The presentation of the information should be quite comprehensible. The system should facilitate the operator's correct conception about the real status of the plant. This can be achieved by clear presentation of the path of influence of an operator (or combination of actions of operators) on the state of the plant. Error tolerant systems should enhance the visibility of human actions in the plant both for the operator himself and the others who monitor his actions. Thus the decisions made by any actor are analyzed and evaluated by a group which greatly enhances the detection of any error. In other words, the group mind checks the correctness of the operators' decisions in view of the instructions and probable outcomes. The linearity of the mechanism of control of the processes by the error tolerant system (i.e. preventing the plant to undergo irreversible changes) enables the operator to take the reverse steps to change the unacceptable error-lead plant status to the initial point of detraction. This feature allows the operator to recover from some committed error through following remedial procedures. The speed of function of error tolerant system must be faster than the rate of deterioration of the plant state due 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 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. According to Roberts & Grabowski (1994) "managers must learn to recognize points in their systems in which desegregated decisions can be tolerated". One solution is an integrated information system that ensures effective horizontal communication that makes the effects of decision 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 other groups.

ERROR TOLERANCE AND ORGANIZATIONS

The concept of error tolerance in organizations requires the management to have a rather different approach to human error. As Debes (1995) has stressed, "human errors are always possible: it is up to the machine, organization and procedures to be forgiving". It is clear that the success of any change or modification in an organization is mostly dependent on the degree of acceptance of top level management. The effectiveness of an innovative system is also dependent on the structural features of the organization. For example, in large tightly coupled, complex organizations, error in one part of the system can propagate to other parts of the system. When organization is tightly coupled, and therefore centralized, it becomes brittle and unable to respond to changing environments. Decision making in tightly coupled organizations is rigid and uncritical. Another example is the quality of

communication in the organization. According to Tanguy (1995), the EDF's former general inspector for nuclear safety, "in most of the operation incidents where human error is involved, I believe there is a problem of communication". The extent of information exchanges within the organization determines the likelihood of misunderstandings between the personnel. Pooling information, sharing ideas, passing on information, drawing attention to something, keeping the shift leader up to date, giving instructions are some of the communication activities which are crucial to team work. Encouraging lots of communication helps the system become more understandable, more linear, predictable and controllable for those operating in it.

The management attitude towards human error has important effect on the acceptability of error tolerance concept into the organization. In learning organizations, when errors are committed, they are mainly considered as a source for improvement. Encouragement of the actors in the organization towards more openness (transparency) and reporting the near misses and incidents without fear of any punishment provides a proper error tolerance climate inside the organization.

Several major accidents have been shown to be structured by a gap between detailed and general knowledge: executives did not have the same knowledge as plant-level managers did. Top level management located far from the plant controls system design, while function managers at the plant keep abreast of the technical details and activities that can put the system in danger. Although we conventionally believe that detailed functional knowledge is "foreign to the normal management tasks" of upper management, only that management level can maintain a systems overview for detecting the "potential for a catastrophic combination" of these threats (Perin 1995).

CONCLUSION

Error tolerance concept is an approach which provides a forgiving cognition environment for the actors to cope with unforseen incidents. The traditional punitive concept of human error has to be reviewed in modern dynamic workstations of low risk high hazard large socio-technological systems in which rapid changes occur in both sides of the system and the human. The adaptive definition of human error has to be incorporated into the managerial practices of traditional hierarchial tight coupled organizations by encouraging transparency and forgiveness towards the error.

ACKNOWLEDGEMENT

Part of the current research has been carried out in the framework of an International Atomic Energy Agency (IAEA) Fellowship Program (IRA/93042P) at Reactor Engineering Division, Jozef Stefan Institute, Slovenia. The authors are therefore very thankful to the IAEA for its support.

REFERENCES

Debes, M. (1995) "*The safety culture policy in EDF nuclear power plants a key for safety and performances*". IAEA International Topical Meeting on "Safety Culture in Nuclear Installations, Vienna, Austria, 24-28 April 1995.

Meshkati, N. (1989) "*An etiological investigation of micro- and macroergonomical factors in Bhopal disaster: Lessons for industries of both industrialized and developing countries*". International Journal of Industrial Ergonomics, 4, 161-175.

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.

Perin, C., (1995) "*How Organizational, Technical, and cultural processes work together for safety*". IAEA International Topical Meeting on "Safety Culture in Nuclear Installations, Vienna, Austria, 24-28 April 1995.

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 Risks and Risk Management. Dordrecht: Kluwer.

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

Roberts, K. H.; Grabowski, M. (1994) "*Some requirements for designing and managing reliable complex systems*". Proceeding of Probabilistic Safety Assessment and Management Conference (PSAM-II), edited by G.E. Apostolakis and J.S. Wu. March 20-25, 1994 San Diego, california, USA.

Tanguy, P.Y. (1995) "The concept of safety culture from a utility viewpoint". IAEA International Topical Meeting on "Safety Culture in Nuclear Installations, Vienna, Austria, 24-28 April 1995.