Unclassified **ENV/JM/MONO(99)12**

OECD OCDE PARIS

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

OLIS : 31-May-1999
Dist. : 02-Jun-1999

English text only

ENV/JM/MONO(99)12
Unclassified

English text only

ENVIRONMENT DIRECTORATE
JOINT MEETING OF THE CHEMICALS COMMITTEE AND THE WORKING PARTY ON CHEMICALS

Series on Chemical Accidents No. 4

REPORT OF THE OECD WORKSHOP ON HUMAN PERFORMANCE IN CHEMICAL PROCESS SAFETY: OPERATING SAFETY IN THE CONTEXT OF CHEMICAL ACCIDENT PREVENTION, PREPAREDNESS AND RESPONSE

Munich, 24 - 27 June 1997
Hosted by the Government of Germany
Sponsored by the OECD Chemical Accidents Programme

78620

Document complet disponible sur OLIS dans son format d'origine
Complete document available on OLIS in its original format

OECD Environmental Health and Safety Publications

Series on Chemical Accidents

No. 4

Report of the OECD Workshop on Human Performance in Chemical Process Safety: Operating Safety in the Context of Chemical Accident Prevention, Preparedness and Response

Environment Directorate
Organisation for Economic Co-operation and Development
Paris 1999

Some other OECD publications related to chemical accident prevention, preparedness and response:

Guiding Principles for Chemical Accident Prevention, Preparedness and Response: *Guidance for Public Authorities, Industry, Labour and Others for the Establishment of Programmes and Policies related to Prevention of, Preparedness for, and Response to Accidents Involving Hazardous Substances* (1992)

International Directory of Emergency Response Centres (first edition, 1992) [prepared as a joint publication with UNEP-IE; under revision]

Report of the OECD Workshop on Strategies for Transporting Dangerous Goods by Road: Safety and Environmental Protection (1993)

Health Aspects of Chemical Accidents: *Guidance on Chemical Accident Awareness, Preparedness and Response for Health Professionals and Emergency Responders* (1994) [prepared as a joint publication with IPCS, UNEP-IE and WHO-ECEH]

Guidance Concerning Health Aspects of Chemical Accidents. *For Use in the Establishment of Programmes and Policies Related to Prevention of, Preparedness for, and Response to Accidents Involving Hazardous Substances* (1996)

Report of the OECD Workshop on Small and Medium-sized Enterprises in Relation to Chemical Accident Prevention, Preparedness and Response (1995)

Guidance Concerning Chemical Safety in Port Areas. *Guidance for the Establishment of Programmes and Policies Related to Prevention of, Preparedness for, and Response to Accidents Involving Hazardous Substances. Prepared as a Joint Effort of the OECD and the International Maritime Organisation (IMO)* (1996)

New OECD Series on Chemical Accidents:

No. 1, Report of the OECD Workshop on Risk Assessment and Risk Communication in the Context of Chemical Accident Prevention, Preparedness and Response (1997)

No. 2, Report of the OECD Workshop on Pipelines (Prevention of, Preparation for, and Response to Releases of Hazardous Substances (1997)

No. 3, International Assistance Activities Related to Chemical Accident Prevention, Preparedness and Response: Follow-up to the Joint OECD and UN/ECE Workshop to Promote Assistance for the Implementation of Chemical Accident Programmes (1997)

About the OECD

The Organisation for Economic Co-operation and Development (OECD) is an intergovernmental organisation in which representatives of 29 industrialised countries in North America, Europe and the Pacific, as well as the European Commission, meet to co-ordinate and harmonize policies, discuss issues of mutual concern, and work together to respond to international problems. Most of the OECD's work is carried out by more than 200 specialised Committees and subsidiary groups made up of Member country delegates. Observers from several countries with special status at the OECD, and from interested international organisations, attend many of the OECD's Workshops and other meetings. Committees and subsidiary groups are served by the OECD Secretariat, located in Paris, France, which is organised into Directorates and Divisions.

The work of the OECD related to chemical accident prevention, preparedness and response is carried out by the Working Group (formerly Expert Group) on Chemical Accidents, with Secretariat support from the Environmental Health and Safety Division of the Environment Directorate. The objectives of the Chemical Accidents Programme include exchange of information and experience, analysis of specific issues of mutual concern in Member countries, and development of guidance materials related to chemical accident prevention, preparedness and response. As a contribution to meeting these objectives, over a dozen Workshops have been held since 1989.

As part of its work on chemical accidents, the OECD has issued several Council Decisions and Recommendations (the former legally binding on Member countries), as well as numerous Guidance Documents and technical reports (see partial list on the facing page). Publications include the OECD's *Guiding Principles for Chemical Accident Prevention, Preparedness and Response*; *Guidance Concerning Chemical Safety in Port Areas* (a joint effort with the IMO); *Guidance Concerning Health Aspects of Chemical Accidents*; the joint IPCS/OECD/UNEP/WHO publication, *Health Aspects of Chemical Accidents*; and the joint OECD/UNEP *International Directory of Emergency Response Centres* (currently being revised by the OECD, UNEP-IE and the Joint UNEP/OCHA Environment Unit).

The Environmental Health and Safety Division produces publications in six series: **Testing and Assessment**; **Good Laboratory Practice and Compliance Monitoring**; **Pesticides**; **Risk Management**; **Harmonization of Regulatory Oversight in Biotechnology**; and **Chemical Accidents.** More information about the Environmental Health and Safety Programme and EHS publications is available on the OECD's web page.

This publication was produced within the framework of the Inter-Organisation Programme for the Sound Management of Chemicals (IOMC).

This report is available electronically, at no charge.

For the complete text of this and many other Environmental Health and Safety publications, consult the OECD's web page (http://www.oecd.org/ehs/)

or contact:
OECD Environment Directorate,
Environmental Health and Safety Division

2 rue André-Pascal
75775 Paris Cedex 16
France

Fax: (33) 01 45 24 16 75
E-mail: ehscont@oecd.org

The Inter-Organisation Programme for the Sound Management of Chemicals (IOMC) was established in 1995 by UNEP, ILO, FAO, WHO, UNIDO and the OECD (the Participating Organisations), following recommendations made by the 1992 UN Conference on Environment and Development to strengthen co-operation and increase international co-ordination in the field of chemical safety. UNITAR joined the IOMC in 1997 to become the seventh Participating Organisation. The purpose of the IOMC is to promote co-ordination of the policies and activities pursued by the Participating Organisations, jointly or separately, to achieve the sound management of chemicals in relation to human health and the environment.

FOREWORD

This report presents the main output of the OECD Workshop on *Human Performance in Chemical Process Safety: Operating Safety in the Context of Chemical Accident Prevention, Preparedness and Response,* which took place in Munich on 24-27 June 1997. The Workshop, hosted by the Government of Germany, was attended by more than 100 experts from 20 countries, including representatives of public authorities, international organisations, research institutes and universities, industry, labour and NGOs. They included participants from Central and Eastern European countries, as part of the continuing co-operation between the OECD and the UN Economic Commission for Europe (UN/ECE).

The purpose of this Workshop was to provide an opportunity for experts from different countries and different sectors concerned with the role of human performance in chemical accident prevention, preparedness and response to consider ways to minimise the number of abnormal events, to control such events when they occur, and to ensure effective response to emergency situations. The Workshop also provided an opportunity to make recommendations concerning best practice.

The first part of the report consists of the Workshop Conclusions and Recommendations. The second part is the Discussion Document, “The Human Element in Operating Safety”. An earlier version of the Discussion Document was presented at the Workshop; it was then revised by the author in light of comments received during or immediately following the Workshop.

The OECD’s Working Group on Chemical Accidents recommended that this report be forwarded to the Joint Meeting of the Chemicals Committee and Working Party on Chemicals, for consideration as an OECD publication. The Joint Meeting agreed that it be should be made available to the public. It is published under the authority of the Secretary-General of the OECD.

The documents in this publication have not been endorsed by, and do not necessarily reflect the views of, the OECD or its Member countries.

TABLE OF CONTENTS

WORKSHOP CONCLUSIONS AND RECOMMENDATIONS

1. The **OECD Workshop on Human Performance in Chemical Process Safety: Operating Safety in the Context of Chemical Accident Prevention, Preparedness and Response** was held in Munich on 24-27 June 1997, within the context of the OECD Chemical Accidents Programme and at the initiative of the Government of Germany. It brought together more than 100 experts from 20 countries, including representatives of public authorities, international organisations, research institutes and universities, industry, labour and non-governmental organisations. They included representatives of Central and Eastern European countries, as part of the continuing co-operation between the OECD and the UN Economic Commission for Europe (UN/ECE).

2. This Workshop was prompted by the recognition that there is a need to study further, and share experience concerning, the role of human performance in chemical accident prevention, preparedness and response. *This is particularly true as advances in technology have reached the point that, in many cases, it is not necessarily practicable to improve safety performance through advanced technology*. In addition, systems are becoming more complex, increasing the concerns associated with the performance of operators and others involved with hazardous installations. The Workshop addressed ways in which human actions can minimise the number of abnormal events, control such events when they occur, and ensure effective response to emergency situations.

3. It was also considered timely to consider issues related to human performance in chemical safety in light of previous OECD Workshops and, in particular, to build on the results of the 1991 Workshop on “Prevention of Accidents involving Hazardous Substances: The Role of the Human Factor in Plant Operations”, hosted by the Government of Japan, and the 1989 Workshop on “Prevention of Accidents involving Hazardous Substances – Good Management Practice”, hosted by the Government of Germany.

Conclusions

General Concepts

4. For purposes of this Workshop, the term "human performance" was used to encompass all aspects of human actions relevant to the safe operation of a hazardous installation in all phases, from conception and design through operation, maintenance, decommissioning and shutdown. The terms "safety" or "safe", as used at the Workshop when describing a hazardous installation or human performance, were not meant to imply that there were no residual risks at the installation.

5. As part of human performance, the concept of "human factors" was considered. Although participants did not agree on a specific definition of the term "human factors" as it relates to operational safety, there was a consensus that it addresses the study of people in the work environment (operators, managers, maintenance staff and others), and those factors which generally influence humans in their interaction with the technical installation (the individual, technology and organisation). The "human factor", for purposes of this Workshop, addresses people critical to the installation and their personal traits, as well as the corporate and cultural context. Issues addressed in the context of the human factor therefore include the selection, physical and mental fitness,

qualifications, education and training, assigned tasks and responsibilities of those involved in operation of the installation as well as management systems, organisational structures, design considerations, and culture in the local area and within the company. These issues are complex and inter-disciplinary and are much broader than simple ergonomics or the man-machine interface. In this regard, care should be taken not to equate human factors only with human errors.

6. The dual aspects of human performance were recognised. On the one hand, man can be a source of error, for example due to the limitation of dealing with several simultaneous, perhaps conflicting, messages and faced with too great a burden of work and/or information. On the other hand, man has the capability to go beyond the automatic capacities of machine systems and represents the last hope to come back from unexpected abnormal situations using manual operations. Humans have the capacity to forecast action, integrate complex and fuzzy information, and understand how to address unusual situations based on experience and training. Therefore, the operator is essential to safety.

7. In addition, it was noted that human errors are not limited to operator errors but may occur at different points in the company hierarchy including, for example, at the level of those responsible for maintenance, management of change, or permit to work systems, as well as supervisors and management.

8. Accidents are generally the final stage of a long sequence of events in which there is complex interplay between technical defects, human error and insufficient organisation/management. Trying to assess blame for past accidents tends to distort the analysis of actual causes. Such an analysis is necessary in order to identify root causes and develop remedies, and to learn lessons so as to reduce the likelihood of similar accidents occurring in the future.

9. Furthermore, while the failure of an operator to follow procedures is often identified as one immediate "cause" of an accident, more in-depth inquiries reveal "root" causes. These could include, for example: the system was not sufficiently error-tolerant; the operator was not adequately trained to address abnormal events; operating procedures were not made available in written form or were not kept up-to-date; the operator was not aware of amendments to the procedures; the procedures were not realistic, or created difficult circumstances or called for illogical actions by the operator; the procedures were contrary to the operator’s conception of the situation; the operator did not have sufficient information or understanding of the malfunction of the system or its cause; the system did not respond to the actions taken by the operator; the process design did not provide the operator with enough data, or provided too much data for an appropriate response to be expected; the operator received unclear or misleading instructions; there was insufficient feedback to the operator; staffing was insufficient; there were cognitive problems in the context of the man-machine interface or between operators; or a reorganisation or change in staff was not properly managed.

10. A number of speakers identified particular "human error" problems which have led to significant numbers of chemical releases. In addition to human failures, these include: problems with transmission of knowledge, especially when experienced specialists retire; the complexity of the system; the ageing of plants and related repairs, without adequate maintenance and inspection; and the need to cope with changes in organisation or technology, including automation. It was also noted that there are particular operating periods in which human errors increase. Such periods include during and after modifications and maintenance, during shutdown/start-up, and following outages.

11. The Texaco explosion and fire in Wales was described, since it produced a broad range of lessons that incorporated a number of important concepts relating to human factors including: the

importance of an operator maintaining an overall understanding of the state of the process at the facility; the difficulty of responding systematically and effectively to multiple alarms; the need to select operators with appropriate personal characteristics, and to provide specific training that will enable them to react responsibly and effectively under stress in an emergency situation; the necessity of updating operating procedures (in particular when a facility is modified); the importance of analysing possible consequences of design changes; and the need to have sufficient supplies of fire-fighting water and equipment.

Safety Culture

12. The ultimate responsibility for the safety of a hazardous installation rests with management. Each individual has responsibility for his/her own safety performance; however, the company has to provide the circumstances in which the individual can act responsibly and effectively. This includes a safety culture in which each employee understands his/her role and has the training and knowledge to carry out this role safely and effectively. It also requires written and understandable operating instructions. Furthermore, operators and others with significant tasks at the installation should be empowered to take the actions necessary to ensure the continued safety of the installation.

13. The safety culture of a firm has a significant influence on the rate of unsafe behaviour and accidents. One definition of an organisation’s safety culture is: the product of individual and group values, attitudes, perceptions, competencies and patterns of behaviour that determine the commitment to, and the style and proficiency of, the organisation's health and safety management. The safety culture derives from the values, attitudes and behaviour of senior management, and the communication of these throughout the organisation.

14. Safety culture is an essential element of process safety management. Inherent in the safety culture should be the dedication by all employees to undertaking their job in a safe manner, following agreed procedures, and assisting their colleagues in meeting these challenges. A successful safety culture requires a top-down commitment to safety, i.e. the visible commitment of top-level executives and managers. It also requires that all employees be aware of the importance of safety. To promote such a safety culture, it has been found useful to provide employees with opportunities to participate in the development and review of safety procedures, and to empower employees to take action consistent with safe operation without fear of reprisals.

15. One important characteristic of an effective safety culture is "error tolerance", i.e. such a culture promotes the capacity of employees to effectively perform their duties and is not focused on assessing blame or punishing errors. In this regard, a safety culture should also encourage an atmosphere of openness in which employees feel comfortable about discussing errors and near-misses in order to improve learning. Thus when an incident or near-miss occurs, management should seek to have an open discussion of the problems encountered and to avoid pressure to attribute blame. An error-tolerant culture still requires responsibility and accountability.

16. As part of their safety management systems, many companies strive to reduce lost-time accidents. It appears that a safety culture that tolerates sloppy behaviour and poor housekeeping (as reflected in a relatively high level of lost-time accidents) is likely to have a culture which does not adequately promote actions to prevent accidents involving loss of containment of hazardous chemicals. However, the converse does not appear to be necessarily true. That is, companies with low levels of

lost-time accidents do not necessarily have a lower rate of occurrence of those rare events with serious consequences.

17. There is also strong evidence that an effective safety management system provides financial benefits to the company by reducing the costs associated with lost-time accidents and shutdowns. Methods are being developed to assess, and provide a basis for improvement of, safety management systems. Such methods/tools should be adapted to the particular circumstances of each organisation. It was suggested that there should be further study to assess how safety culture and safety management systems affect the level of significant accidents.

Design Issues

18. The conception/design of hazardous installations needs to recognise the real possibility of human error and take into account the psychological, physiological and cognitive capabilities and limitations of people who have significant tasks at hazardous installations. Concept design should take into account means for making the actions required by operators relatively easy, reliable and consistent with the cognitive abilities of operators, and thus minimise errors. The operating concept/procedures should document the safety features incorporated in the design, including automated safety systems, as well as the role of operators, managers, maintenance staff and others.

19. To avoid designing a facility that has latent operating errors, tests should be used to determine whether the operating design is feasible (including consideration of whether it adequately takes account of the limited quantity of information that can be processed by humans under the conditions which might be faced by the operators). In light of the potential for information overload, further efforts are needed to test systems to determine the possibility, and implications, of such overload and how changes in design, organisation and management can address this issue.

20. In addition, in designing systems there should be safety analyses to address abnormal events which are anticipated, as well as to provide a means for operators to address those abnormal events which were unanticipated. It is important that the design allows for the possibility of human intervention under abnormal circumstances (recognising that automated safety systems may be triggered).

21. Good design needs to be combined with proper safety management systems, including: training and education of employees; appropriate development, implementation, review and updating of operating procedures; careful management of design changes; consideration of the implications for safety when there are employee or management changes; and audit and control procedures.

22. Trained individuals tend to be reliable in abnormal situations, especially when reasonable recovery time is available. Therefore, in order to reduce the failure rate of a system, its design should allow a certain amount of time for the operator to react in abnormal situations. (As an example, it was noted that 30 minutes is the norm for reaction time in the nuclear sector, whereas for aircraft reaction time is measured in seconds; chemical plants are somewhere in between.)

23. Modern computer systems are important to operating safety. Systems should be designed to predict and document possible event scenarios, including frequencies and possible consequences, and to facilitate emergency planning. In addition, on-line systems should support operators in carrying out their responsibilities, and in providing easy and rapid access to operating procedures and related information. On-line systems should also be able to capture information useful in determining the

root causes of incidents, while off-line systems should provide easy and rapid access to documentation on the company, for emergency planning and for training of employees.

24. An appropriate level of automation, and decision support systems, should be incorporated in the design of a hazardous installation. It appears that full automation is neither realistic, nor optimal, from a safety perspective. While automation and decision support systems can increase safety due to rapid diagnosis and response, such systems only address known abnormal events. Those events which are not within the design specifications, or which were not predicted, need to be dealt with manually (information systems may be very helpful under these circumstances). Thus the presence of an operator who is well-informed and well-trained to respond is indispensable.

25. While automated systems are often useful for improving safety, it was noted that there are limitations to their value. For example, if a process is automated to the extent that the operator has very limited responsibilities, he/she may not be sufficiently aware or experienced to handle the rare abnormal conditions. Safety can also be compromised if the responsibilities of the operator become too routine, or if the operator does not have sufficient opportunities to utilise his/her skills. Furthermore, the value of automated systems requires that the operator be signalled when automated safety system(s) are triggered, and that he/she has information concerning the actions taken through the automated systems. The operator should be well-trained on the meaning of signals and their implications.

26. It is important that systems designed to ensure safety, whether automated or requiring human intervention, cannot be overloaded and therefore fail to work. For example, consideration should be given to what might happen if several systems in the installation failed at the same time. Would the operator be inundated with signals and therefore be unable to distinguish among them (or to process and understand information) and so be unable to determine an appropriate course of action? Automated systems should be designed so that the more important signals get through to the operator, especially when several automated systems may be triggered simultaneously. It is critical to take into account the possible psychological effects on an operator when systems fail, and how such stress will affect the operator’s ability to react.

27. Efforts are under way in some countries to promote a concept of "inherently safer" process and installation design in order to reduce risk and increase safety, health and environmental (SHE) protection. Use of this concept has been shown to lead to improved SHE performance, reduced capital and operating costs, and improved operability and reliability. It is generally agreed that the principles involved in inherently safer designs are valuable in promoting safety because safety performance is less reliant on "add-on" engineered systems and management controls. However, there is no consensus concerning the definition of the term "inherently safer" in the context of the design of hazardous installations, especially as the term is translated into different languages. Similarly, different terms (such as "intrinsic safety") are used to describe similar concepts.

28. Inherently safer approaches involve careful selection of the process, along with good design of the installation (in effect, designing out certain hazards, minimising the effects of human error, and better tolerating errors which might occur). Such approaches utilise the following concepts, to the extent that they decrease overall risk:

- reducing inventories of hazardous substances;
- replacing hazardous materials by less hazardous ones;

- using hazardous materials or processes in a way that limits their hazard potential (e.g. through closed systems);
- making the plant and process simpler to design, build and operate; and
- shifting complex systems to more linear ones.

29. Care should be taken to ensure that design choices or modifications do not inadvertently increase or transfer risk. For example, in some cases reducing inventories of hazardous substances may increase overall risk due to the greater need to transport the substances. Thus the benefits in terms of risk reduction should be identified and documented.

30. It was recognised that implementation of the concepts in paragraph 28 alone does not necessarily lead to an inherently safe plant; as long as there are hazardous materials in a facility, there is the potential for accidents. Furthermore, the principles of inherent safer design should not be used in isolation but rather should be part of an integrated approach to safety. This involves operation and maintenance of the installation, and the application of management systems, in a manner consistent with safety. Considerations involved include: ensuring the continued integrity of equipment over time; personnel management; management of change (e.g. with respect to staff, design, production); training of operators and other employees; reviews and audits of safety performance; and learning from experiences such as analyses of accidents and near-misses. Also included is the establishment of a culture within the company, with a top-down commitment from the highest levels of management, that promotes and rewards safe practices.

31. The term "inherently safe" as well as the term "inherently safer" can cause confusion, particularly among the general public, in light of the implication that a facility which has been designed in a manner consistent with this principle does not pose any risk. While such a facility may have a lower level of risk, there remains some risk which should be subject to assessment. Therefore, it is important to ensure that these terms are used carefully and that the risks posed by the facility are properly understood and communicated.

Operating Practices and Procedures

32. It was suggested that, within companies, the integration of management systems for environmental, health and safety issues and the development of company-wide procedures applicable to all sites lead to improvements in process safety. The use of such procedures can help to identify situations which could result in occupational injuries, as well as more serious organisational failures or other errors resulting in releases of hazardous substances.

33. All hazardous installations should have in place appropriate written procedures which can be understood by relevant members of staff. In addition, at all such installations there should be education, training, review and monitoring systems for ensuring that all staff know, understand, and follow at all times appropriate procedures, and that these procedures are periodically reviewed and updated to take into account any significant changes in plant design or operation. Operators, maintenance staff and others with significant tasks at the installation should be involved in the development and maintenance of procedures. This helps ensure that procedures are realistic, workable and consistently applied, and facilitates the idea that those who have to follow procedures

"own" them. Furthermore, all appropriate staff members should be made aware of any modifications to the plant.

34. Efforts should be made to ensure that personnel are informed of, and participate in, activities concerning their work environment, including, for example, maintenance, testing and calibration. In addition, they should be involved in related activities such as design of work areas, risk assessments and audits of facilities. Towards these ends, personnel should be trained to make their involvement meaningful.

35. A contemporary issue relates to manning levels, in light of efforts to reduce the size of enterprises and move to more horizontal organisations. This issue relates not only to the operator, but also to supervisory and management personnel. Reductions in staff size do not necessarily affect the level of safety since other factors are involved, including design, management and operation. However, it is possible that staff cuts can lead to reduced safety communications, a disconnect between policy and hands-on action, and less time for training, voluntary inspections and time-off between shifts. Furthermore, they have safety implications because of the loss of experience and the increased number of cases of operators working alone rather than with a team. On the other hand, combining staff changes with other types of changes sometimes has a positive effect on safety. Current methods of calculating manning levels include workload and time-line analysis and industry experience. Additional research is needed to improve understanding of issues related to manning levels and safety.

Staff Qualifications and Skills

36. It is important for employees at all levels to accept responsibility (and be held accountable) for carrying out their tasks, both as individuals and as part of a team. Experience indicates that when an organisation gives operators responsibility in an atmosphere of trust, and provides the tools needed, individuals make decisions, and perform, better than one would expect.

37. Operators should have an overview of the activities in the installation. If an operator has such an overview, he/she is better equipped to respond to abnormal events; when automatic safety devices are triggered, the operator is aware of which systems are operating and the overall state of the installation. In this regard, advanced computer systems can give a global picture of the state of the plant and assist operators in abnormal or emergency situations.

38. Operator perception, especially with respect to making decisions in an emergency situation, is an important factor in operational safety. Perception draws on previously acquired information and existing understanding of the system; thus it can be complex, uncertain and subject to numerous ramifications. Exercises carried out should be sufficient in number for operators to understand emergency situations and react properly.

39. The importance of training and educating operators and others working at hazardous installations was emphasised, both in terms of initial training for the job and continuous training to ensure that employees remain aware of the procedures to be followed, any changes that might have occurred, and actions to be taken when incidents occur outside system design. To be effective, training should be in a language that personnel can understand and should provide information concerning the overall nature of operations, as well as specific information related to each individual's

responsibilities. Effective training programmes are designed to help employees understand, *inter alia*: the plant; procedures; possible deviations from normal conditions; possibilities for other abnormal situations; and strategies for recovery in abnormal situations. Personnel should be trained with respect to all aspects of risk prevention and mitigation.

40. The nature of the training and education needed should be analysed, and training and education programmes should be monitored and evaluated for effectiveness and revised as appropriate. Many companies are now analysing the interrelationship of the man-machine interface to determine the priorities for training opportunities.

41. In developing and implementing training programmes, consideration should be given to the most effective methods of training in particular circumstances. For example, operator-to-operator training has been shown to be effective, as have on-line systems and electronic simulation models. Training programmes should be designed to instil in operators the confidence to question the decisions of senior personnel, or of automated systems, when they believe this is important for safety.

42. It was noted that it is increasingly difficult to acquire and practice manual and cognitive skills, and to retain the process knowledge, needed for correct application of diagnostic and corrective actions in the operation of modern automated systems. The use of simulator training provides a means of addressing these situations. Even though every facility has its unique characteristics, which may imply that simulation training must be custom-made for each application, there are models available for various unit operations. These are available in many combinations to teach trainees how to perform basic operations and to address abnormal situations. Recent simulator training concepts may also be performed on remote workstations with on-line access to training centres. This could be a low-budget option of particular interest to small and medium-sized enterprises. It was recognised that much research is needed in order to optimise the use of simulators.

43. Workshop participants emphasised the need for improved education and training of engineers and others responsible for the conception, design and construction of hazardous facilities, so that they will better understand the importance of safety, health and the environment and the principles involved in inherent safety. It was recognised that universities in some countries have started to incorporate these concepts in their engineering curricula. However, further efforts should be made to more broadly incorporate the subject in technical schools and universities in a meaningful way, which would allow students to understand the need for SHE to be integrated into general engineering concepts (and not only to be considered separately).

44. Larger companies, trade and professional associations, and others also have an important role to play in promoting safety concepts and providing training. It was noted that there are courses available to train qualified engineers through special training centres and institutions which register engineers.

45. Even when operators and other employees are well-trained, informed, and motivated in a good safety climate, it should be recognised that they could be restricted by physiological and psychological limitations. Among the factors influencing human performance, the willingness to perform is the most important along with physiological capacity and skills. Factors such as individual perception, group thinking, self-protection, and loss of good will also have direct impacts on how employees function. It is very difficult to measure or predict how such factors will influence a particular situation.

Regulation and Compliance

46. Representatives of a number of countries, as well as the European Commission, described their regulatory systems and administrative practices designed to improve safety. Common approaches included the requirements related to identification and registration (notification) of hazardous facilities; risk assessment; the development of safety management systems; emergency planning and accident reporting; information to the public; enforcement (inspection and control); and documentation of the underlying operating concepts.

47. Regulatory authorities have a role in promoting process safety by providing guidance material on, for example, the evaluation of safety management systems to determine where further work is needed. Such guidance material, as well as guidance prepared by professional associations, can help SMEs to establish programmes as well as to evaluate their progress.

48. There may be a role for third-party organisations, including industrial safety institutes, auditing organisations and others, in assessing the safety management systems of individual installations, not only to ensure compliance with regulatory requirements but also to identify shortcomings which could be addressed through training.

49. Further efforts should be undertaken to determine how insurance companies could provide economic incentives to improve safety performance (e.g. through decreased premiums), based on the results of safety audits, good safety practices and/or increased use of safer design principles. Insurance companies should develop the capacity to undertake safety audits and reviews of safety practices and designs.

Internal/External Communication

50. Effective communication among management, other employees, and contractors working within a hazardous installation is necessary. The benefits of dialogue between the facility and local authorities are increasingly being recognised. Care should be taken to ensure that important communication linkages are not blocked by, for example, language differences or a presumption that employees or contractors do not care or cannot understand relevant facts.

51. The importance of providing active and passive information to the public concerning hazardous installations, and participation of the public specifically in preparation of emergency plans, was stressed. It was noted that a well-informed public can directly lead to improvements in accident prevention, preparedness and response. In this regard, the public should not only have access to information provided to public authorities about the hazardous installations (passive information) but should also receive information, in the form of brochures or leaflets, about the products and releases which may pose a risk to the public, as well as about appropriate behaviour in emergency situations (active information). The aim should be to engage the local community in a dialogue before an accident takes place, leading to the development of partnerships and the building of trust. This is particularly important in the context of emergency planning. Provision of information to the public is the joint responsibility of public authorities (including local authorities) and the relevant companies.

52. Experience has shown that significant benefits accrue to companies which reach out to the community and provide opportunities for two-way communication. Furthermore, a well-informed public will understand what actions to take in the event of an emergency and will be more likely to follow instructions. The ability of the public to understand issues which may have some technical complexity should not be underestimated.

53. Communication within the facility, and with authorities and the public, can be driven by regulatory requirements such as community right-to-know, by industry associations' initiatives (e.g. Responsible Care in the chemical industry), or by a particular company's interest as a partner in the community.

54. Systematic analyses of past accidents, incidents and other deviations can be of great value and should be undertaken. This will involve gathering of all relevant information on the deviations and their context, and careful analyses by teams that bring together all the relevant skills and experience. This will facilitate comparison of results and learning of lessons from past accidents.

Recommendations

55. The Workshop reached agreement on the following Recommendations for future action. In many cases the Recommendations do not identify a particular party or group that should take responsibility for following through on the actions described. Nevertheless, the Workshop concluded that the Recommendations are very important for improving safety, and therefore that further consideration should be given by the OECD and other fora to how the desired objectives could best be achieved.

56. Further research is needed concerning how operators and others perceive, understand and react to normal, abnormal and emergency situations. Furthermore, there should be additional development of models or methods to explain the influence of various factors on human performance and to improve understanding of the cognitive process. Among the issues which should be addressed are:

- how operators react to multiple warning signals;
- which signals are most likely to elicit appropriate responses;
- how operators react to abnormal events which have not been predicted; and
- other limitations in information processing by humans under the stressful conditions which might be faced in an installation under abnormal conditions.

57. Further research should also be undertaken on the effectiveness of safety management systems and corporate safety cultures, including means for measuring safety.[1] Specific issues to be considered include: how to improve management decisions concerning manning levels; and how to achieve an

[1] The Workshop suggested that ways are needed to measure safety management systems and safety cultures proactively, so as to increase levels of safety and reduce the likelihood of accidents. Examples of rates or indices used to measure safety performance are:

- accident frequency rates (e.g. deaths and injuries per million man hours);
- accident severity rates (e.g. lost working days per thousand man hours).

appropriate balance, in a given situation, between automation and involvement of the operator. Such research should include a review of industry practices.

58. Management should take measures to help avoid the situation in which jobs which are critical for safety become too routine or too limited in responsibilities. This can be done, for example, through careful planning of shifts (taking into account, for example, the skills of the operators) and by rotation of jobs.

59. Given the increasing use and sophistication of computer-based systems, research should be undertaken on how such systems can be used to improve safety in design and operation of hazardous installations and improve training of operators and others in such installations.

60. Increased efforts should be undertaken to improve understanding within industry and public authorities of the concepts involved in "inherently safer" designs. The main obstacles to increased use of such concepts appear to be a general lack of awareness or training, a lack of sufficient tools and methods, the need for hard proof of the benefits of such concepts, and a general conservatism in the design/engineering community (preferring to use designs which have been used in the past). In addition, in order to use these concepts, safety issues should be considered early in the project conception and design. Furthermore, there appears to be a concern that, in some cases, the need to meet regulatory requirements preclude the use of some of these concepts.

61. Further efforts are needed to develop methods and means for describing operating concepts.

62. Efforts should also be undertaken to develop means of demonstrating the financial implications of applying appropriate safety cultures and safety management systems (given the understanding that these result in financial benefits to companies).

63. Public authorities, industry associations and others should improve the sharing of guidance materials related to human factors and safety management systems and, more generally, to improving safety, health and environmental performance of hazardous installations. Systems should be established to facilitate such information sharing on a voluntary basis.

64. In light of the continuing concern about small and medium-sized enterprises, concerted efforts should be undertaken on a co-operative basis to improve communication with, and assistance to, SMEs. One specific area discussed was how to improve training at SMEs, perhaps using computer-based technologies. Public authorities, trade associations and larger companies (consistent with principles of product stewardship and Responsible Care) should participate in this effort.

65. While there have been improvements in the education and training of engineers with respect to safe operation of hazardous installations, further efforts are needed. Improved safety training of chemists is also needed. Tools for teaching safety matters to engineers, chemists and other concerned disciplines should be developed, after an analysis of the needs in this area.

66. Regulations should be reviewed to see how they might hinder the use of improvements in design (such as those described with respect to the concept of "inherently safer" processes). In addition, regulations should be reviewed to see if they require the use of superfluous add-on "safety devices" that have become unnecessary as the result of design changes.

67. Industry should be encouraged to open a dialogue with local communities and their representatives, in order to ensure that the potentially affected public is well-informed about the processes being

undertaken at hazardous installations, and about accident preparedness and response. Specifically, companies should be encouraged to invite local citizens for tours and presentations in such installations and to set up community liaison groups.

68. Further efforts are needed to collect, analyse and share incident data. This should be done in a structured way, in order to provide meaningful information and comparable results and make it possible to learn from experience. Lessons learned from accidents and near-misses should be collected, evaluated and distributed in a systematic way.

69. Management of hazardous installations, industrial organisations, public authorities, and others should consider how to create a climate that fosters trust and encourages voluntary reporting and sharing of information. In this regard, further efforts should be made to analyse the root causes of accidents as well as for companies and public authorities to share such information.

Discussion Document:

The Human Element in Operating Safety

Joseph Fragola[1]

Introduction

Human actions have always been critical to the safe operation of systems. Despite advances in automated systems, humans are likely to remain essential to safe systems operation in the future because of their inherent flexibility in recovering from unique potential accident situations. It is this flexibility which makes it advantageous to include human operators in system designs. However, designers realise that the same human characteristics which enable this flexibility also bring about the fallibility that is often identified as the cause of accident initiation. Humans have unique abilities which enable forecasting from the known to the unknown, the use of stereotypical cases to rapidly narrow the search space, and the incorporation of sensory information in a holistic way. All of these features, which are the hallmarks of expertise in action, can also lead directly to incorrect action. For this reason, the human contribution to the risk of system operation has always been claimed to be significant. Further, as system hardware becomes ever more reliable, and systems become even more complex, the claims of human contribution to risk are likely to rise at least proportionately.

While percentages may vary from industry to industry, it is probably fair to say that the majority of accidents at the current time appear to be initiated by humans. This situation has resulted in a call by some to resort to more and more highly automated systems. On the other hand, it is also probably fair to say that in cases where accident conditions exceed the range of historical expectations, the operator has been the only hope for recovery and has often performed remarkably well in averting the consequences or diminishing the impact of potentially serious accidents. This dilemma has been recognised by even the most ardent advocates of fully automated systems, who inevitably include an operator in case something goes wrong that the automated system cannot handle. Additionally, appearances can be deceiving. In many cases, events which might appear to be the result of human error are actually the result of the operator being placed in a decision-making environment within which error becomes likely, even foreordained. In some cases, the designed operational environment or the pressure of the cultural environment can burden the operator’s decision-making to the extent that errors are to be expected. In these situations, the initiation of undesirable events then seems more properly the responsibility of the designer or the managers responsible for establishing and maintaining the operational culture.

Those who continue to advocate fully automated systems are still faced with the issue of demonstrating their claims of high levels of safety. In order to do this, the designer runs directly into the

[1] Science Applications International Corporation, New York. The Discussion Document was prepared for this Workshop. It does not necessarily represent the views of Workshop participants.

analogous problem of proving the claimed high reliability levels of the software upon which the systems are based. Recognition of this problem of reliability demonstration has caused some designers to incorporate only “highly field-proven” software in their designs, contending that the previous field trials have demonstrated its reliability. While this strategy might be adequate for static designs, the reuse of field-proven software in new designs, even designs which are generationally similar, is so fraught with difficulties (as the Ariane V launch vehicle designers have learned so painfully) that some developers advocate that previously developed software should never be incorporated in designs requiring high levels of reliability. Further, while relatively simple automated systems might demonstrate high levels of reliability operating in well-understood environments, this does not necessarily imply that they will remain reliable, as the operational environment changes even if the hardware remains the same, as the hardware ages, or as it is affected by human interaction as a result of maintenance.

Once it is agreed that the operator is an essential element in safety, the objective should be to minimise the number of human errors which will occur, to limit the impact of those which do occur, and to maximise the effectiveness of the operator in dealing with safety-significant events when they do occur, however they are initiated. Reducing the number of errors requires that the operator and his operational environment are carefully taken into account. This implies not only the development of an understanding of the machine-related operational requirements and anthropometric capabilities, so as to design an operator-friendly machine interface, but also of the cultural environment in which the operator is immersed. This cultural environment, which is sometimes ignored, often plays a critical role in developing a proper safety consciousness on the part of the operator. The concept of “culture” certainly includes the local community culture and broader-based regional cultural characteristics, but it also and perhaps more importantly includes the culture established in the plant by its management through its system for rewarding and punishing actions. Limiting the impact of the errors which do occur involves the establishment of operational and emergency procedures and levels of protection within the system design, as well as operational training in these two important accident-mitigating features. Training and the associated training materials and tools are also important in the development of effective operational responses when, despite all efforts, potential accident sequences are initiated. Effective operational response is also significantly affected by the selection and assignment of operational personnel, based upon their inherent capabilities and previous background as well as their experience operating the particular system or process at hand.

Balancing Automation and Human Action

Given the dual influence on safety of human participation in control of systems, there is general agreement that a balance needs to be drawn somewhere between automation and human control. There also appears to be a consensus that automation increases the safety level by allowing rapid diagnosis and automatic response to known abnormal events (so-called “normal” abnormal events). However, there is also general agreement that automatic systems fail miserably when they are forced to address events whose characteristic operational parameters are outside the space of parameters considered in the specification (so-called "abnormal" abnormal events). Therefore, some human participation in control will always be required.

It would be useful to consider how the proper balance between automation and human action might be established and what role, if any, the historical record on common or similar systems should play in the decision.

In this regard, industry should evaluate whether increased automation in control has been, in general, a good thing, and whether in the chemical process industry in particular the current level of automation is too low, too high, or about right. If more automation is required in order to increase the level of operational safety, then some measure should be established to determine how much is enough. In addition, if more automation is planned, then consideration should be given to how the safety of operator actions can be ensured throughout the transition. Another issue whose importance should be considered is the means for maintaining operators' skill levels such that they can respond to circumstances outside the state space of the automated system, particularly when they are being converted ever more into the role of system supervisors rather than system operators.

Responsibility for Correct Human Performance

Statistics seem to back up the assertion that the majority of accidents are caused by humans. However, some researchers would clarify this assertion by suggesting that the operator is just at the end of a long train of previous actions and that the seeds of accident initiation are often planted in the systems well before the operator ever gets involved in its operation. Some researchers have described so-called "latent" error situations as error-likely, even error-compelling. These situations have even been compared to disease-causing "resident pathogens" which remain hidden in the body of the design until a peculiar confluence of events activates them from their dormant state, i.e. to be the actual cause of the accident, which is then unfairly charged to the operator.

It is possible that the operator is too often blamed for design errors which, upon objective review, would be highly likely to result in errors in operation. If this situation is true today, then the future impact on error likelihood of current trends in design should be assessed. But if human errors are to a degree ultimately linked to errors in design, there exists a potential excuse for the operators to deny their legitimate responsibility for safe operation. Blaming designers could be sending an incorrect message to operators.

Inquiries into blame and responsibility subsequent to the occurrence of an accident can either be seen as legitimate or as counter-productive searches for scapegoats. However, if such inquiries are abandoned, then the issue of incentives for operators to take their safety responsibilities seriously comes into play.

Some evaluation is needed as to what a designer can legitimately be expected to consider and address in design development, as it relates to operational safety performance.

If it can be said that there are legitimate operational regimes where the operator can properly be held responsible for accident prevention, then decision-making is required on how these regimes can be determined and how they should vary with the type of design being operated; with the resources, personnel and public population at risk; with operator pay scale; and with educational or licensing requirements.

Operational Burden as it Relates to Operating Safely

Since human short-term memory is limited, even skilled operators can be placed in error-likely situations if enough competition for their attention is imposed upon them by the operational environment.

There is some evidence that experts can be shown to perform no better than novices if they must attend to more than two competing events at the same time. In some cases, the stressfulness of a situation has been seen to cause operators to take actions, even actions which may place them at great personal risk, in order to exclude outside distractions from competing with the task at hand. Conflicting signals presented to the operator by the design have been shown to cause similar effects, as have conflicting policy signals from management. Management has a dual responsibility: the responsibility to corporate upper management, and ultimately to stockholders, for profitable operation, and the responsibility to personnel and the public for safe operation.

There are legitimate concerns as to how management can properly balance these two responsibilities and send consistent signals to its operational staff. Thus it is advisable to make some assessment of the role an analysis of a facility’s design and its operational history can play in determining this balance.

If the increasing complexity of operated systems places more burden on operators, then the role of automation in the form of operational aids in reducing the operational burden should be assessed, as well as the role of training and procedures in this regard.

In the face of corporate downsizing and associated reductions in maintenance and operational staff, there may be steps management can take to prevent the development of a burdensome environment. For example, it might be possible to measure the effectiveness of human resources benefits, such as counselling services, in the reduction of personal stress levels which could contribute to operator burden.

Maintenance and Scheduling Burden and Operational Safety

The demands imposed by the operational environment and the possible conflicting signals generated by the design or by management are not the only activities which place a burden on the operational staff. Burden is also caused by the requirement for the operations team to perform duties outside the traditional operational role. For example, since the operations team is primarily responsible for operational safety, they must ensure that the proper system state exists before, during and after required activities of other members of the operating staff (such as in-service inspection, maintenance and calibration). This implies not only that they must be responsible for understanding what state the system is in, so as to minimise the possibility of these activities initiating an accident, but also that they are responsible for ensuring that the equipment being addressed is properly “cleared”, continues to be cleared while the activity is ongoing, and is properly restored afterward.

There are several options for the assignment of these responsibilities. For example, a member of the active operations team, or others in the operational staff, might be assigned these tasks, but not those on the line operating team. In the case of reassignment, consideration should be given to how the operators making the active control decisions can remain cognisant of the plant state and the available equipment set.

An identification of the proper division of responsibility between the line operational staff, the maintenance staff and plant management in this area is needed, specifying particular tasks to the extent possible. It would also be useful to identify whether operational aids would be of assistance to reduce the burden on the line operators for those tasks which must remain their responsibility.

Corporate Safety Culture

The culture that surrounds the operation of a facility has a significant influence on safety. This culture includes not only national and regional characteristics, educational backgrounds and standards of living, but also, and perhaps more importantly, the culture present in the overall corporation and specifically in the operational facility itself. Problems can also develop where these two cultures clash. The popular literature is full of examples of corporations, whose corporate roots are imbedded deeply in one society with a particular cultural heritage, trying to transfer their successfully developed corporate culture based on that heritage to another society and failing miserably in the process. Rigid culturally-based corporate programmes, including safety programmes, may not be transportable to more flexibly-based societies. On the other hand, all flexible programmes may be misunderstood or disrespected in more rigid societies. Safety culture and its role in operational safety has recently become a “hot topic”.

It is not possible to evaluate the importance of safety culture without first defining it and determining whether and how it can be measured. Otherwise, it may just be seen as another management idea with a short life-span. This definition should address whether there are generic characteristics of a good safety culture that span national, regional, societal and corporate boundaries and, if so, what they are.

If certain types of corporate environments can be identified as being more or less prone to the establishment of a good safety culture, then there may be the possibility that safety culture can be taught rather than believing that a safety conscious attitude must be innate to the corporate environment.

Labour and Management Issues

Labour and management both have a stake in establishing a good safety culture. Whether the labour force is organised or not, accidents can have significant consequences on the health, safety and careers of the plant operational staff. Therefore, safety is an important issue to them. Moreover, accidents affect productivity and therefore the careers of plant managers. In some nations, these managers are even held personally and criminally responsible for the safety of the labour force under their charge. However, these natural safety consciousness forces can sometimes be diminished when the threat of an accident is seen as remote and safety requirements challenge immediate profits for management, or impose apparently undue and unnecessary burdens on the labour force. Further, the cost of a good safety programme must come from somewhere and corporate profits, or labour force incomes, are often perceived as the likely sources.

There is some question as to whether labour unions constitute a positive force in the establishment of safety culture because of their concern for their membership, or are a detriment because of the economic pressures they might place on management and the resulting competition for scarce corporate funds which might be needed for safety.

Given the natural tension between labour and management if the labour force is organised, the role that labour organisations (such as labour or trade unions) play in the establishment of good safety culture is a key issue to consider, particularly with respect to labour and management relations.

It would be interesting to evaluate whether plant operational personnel should be able to establish the balance between their own personal safety level and their personal income and, if so, how this should be achieved.

“Inherently Safe” Designs

Designs which by their very nature reduce the risk of operation and maintenance are certainly to be preferred to alternative designs. However, any assessment of inherent safety implies a determination before the fact with a limited, and to at least some degree inapplicable, historical data set. In the past, commercial aviation aircraft designs with a larger number of engines were deemed inherently safer than those with fewer. In the US, early designs were required to have at least three engines to be considered safe enough for passenger transport. However, one of the safest designs to evolve in that era was the two-engine DC-3, which became the mainstay of US commercial passenger transport for many years. More recently, the US restricted transcontinental passenger traffic to at least tri-engine craft, but this raises questions as to whether the dual-engine designs now in service have proven any less safe than three and four engine craft of a decade ago. In the nuclear power industry, early reactors which used natural convection cooling and gravity-fed isolation condensers were once thought to be inherently safer than alternative designs which incorporated active cooling stand-by systems. Then along came the concern for seismic vulnerability, and designs with elevated water sources appeared less safe and were abandoned. In the East, there was so much concern for the design basis loss of coolant accident that a design was developed which essentially eliminated that event from the design basis, but the inherent safety of these RBMK 1000 units is highly questionable given their operational safety record.

Among the issues to be considered relative to design improvements are whether passive safety systems are inherently safer than those which employ more active systems, and whether automated active safety systems are inherently safer than those which employ some manual intervention.

A fielded design that has operated for several decades is likely to have been modified so as to be robust against its operational environment. Its operators have usually developed procedures to address its operational limitations, and its maintenance crews usually know what it takes to keep it running safely. In general, the operational and maintenance environments are much better understood than that of a new “paper” design. One could then legitimately question whether a design with a broad base of experience of safe operation is inherently safer than a hypothetical new design. For this reason, there must be a means for comparison between a safe design currently operating and a new paper design which promises even greater safety, in order to permit logical decisions to be made. Pilot plant or test programmes provide insight to new design efficacy, but it is appropriate to ask when enough operational experience can be considered to have been accumulated to allow deployment of a new design. Further, at that stage an assessment should be made as to whether, and what kinds of, actions can be taken before and during deployment to ensure that the residual uncertainties that may lie unknown in the bowels of the new design are addressed.

These issues bring into question the respective roles of historical data, experience, judgement, intuition and analysis in the design decision-making process and how they can all be blended together.

Establishing a “User-Friendly” Environment for the Operator

A great deal of discussion in the literature base related to operated systems is directed at the development of user interfaces which are “user-friendly”. The term has developed a broad definition, but is usually defined to be related to the design of an ergonomically designed man-machine interface. That is, the designers have taken into account the range of internal resources available to the human element of the system and have attempted to design the interface in recognition of these resources, rather than expecting the operator to adapt himself to the system as designed. However, the development of interfaces which are user-friendly according to this definition may often mean that a human factors specialist back in the designer's facility is deciding what is best for the operator. User-friendly designs based upon experiment and not operational research can sometimes fail to be friendly at all, because in the final analysis it is the operator-user who decides if the interface is friendly or not.

A thorough consideration of this issue involves the elements of the operational and maintenance interface which are candidates for user-friendly revision, and the role the operations and maintenance team should have in establishing a user-friendly operating environment.

The virtual control room concept (wherein controls and displays are themselves computer generated and displayed rather than hardware implemented) may also play a part in a user-friendly operations environment, as can the Personal Control Room concept, wherein each operations team can tailor the operational interface to its own needs.

Given the possibility of customising the operator interface, the potential safety enhancements involved in the user-friendly reconfiguration of the control and display interface based upon plant state (i.e. start-up, normal operation, emergency response) should be addressed.

Safety audits, control room design reviews and other qualitative approaches have proven to be powerful verification tools, as well as powerful tools for identifying deficiencies in the operating and maintenance interface. However, decision-makers must still establish priorities in addressing deficiencies within a constrained budgetary environment, and this may not be consistent from one industry to another.

It has been suggested that maintenance and calibration teams have been the forgotten stepchildren in the safety of operation. It would be worthwhile to identify the availability, and evaluate the appropriateness, of user-friendly aids to address problems encountered in ensuring the correctness of maintenance and calibration.

Physical and Psychological Resources of Plant Operators

The plant operator functions as an integral element of the plant control system. By attending to sensory inputs from the plant instruments, he or she is expected to process these inputs internally and initiate the bodily outputs appropriate to the input. These bodily outputs might include interaction with other plant instruments, or the initiation of discussions with other plant operators, other members of the plant operational and maintenance staff, or plant managers. These discussions might be directed at obtaining further information to determine whether and/or what action might be required, or to solicit the validation of an intended action with either a broader experience base or as consistent with plant policy and operating procedures. Bodily outputs also might include interaction with plant controls, with the intention of bringing the perceived plant state more in accord with what is considered to be the correct one under the existing operating conditions and environment. Ultimately, except in the rare cases of fully automated systems, the operator "closes the loop" to ensure proper and safe operation.

Even presuming that the operator is operating the plant in good faith, there are finite limits to the resources that he or she is able to bring to bear during each interaction with the plant and during each step in the interaction process. These limitations can facilitate, and in some cases force, missteps. For this reason, designers and plant managers need to ensure that operating requirements do not push towards the envelope of the limits.

Consideration should be given to the variety of sensory pathways that are reasonably available (or could be in the future) for operator data acquisition and command intervention, for the spectrum of plants that currently exist in the world-wide chemical process industry, and the commensurate limits of information intake via each of these pathways. It should be recognised that these limits would ultimately have to be stated in practical terms to be used as design guidelines by the non-expert designer or manager, so that they may be careful not to overly constrain or prevent the pathway’s use altogether.

Gains in information acquisition might be possible via pre-processing, since human sensory input resources are fixed and limited. Still, the limits to these gains themselves should be addressed.

Even if the human data acquisition system were unlimited, operator effectiveness in action would still be limited by the human information processing system. This system is usually described as having two major components: Short Term Memory (STM), which is extremely limited in storage capacity but rapidly accessible, and Long Term Memory (LTM), with an essentially unlimited storage capacity but much slower access. Discussion is needed to identify what these limits imply in practical terms, and whether (and in what way) automated operational aids or procedures could be of assistance in overcoming them.

Underlying Psychological Basis for Human Factors and Human Reliability Models

A large body of work exists related to the subjects of ergonomics (or human factors technology) and human reliability analysis. In fact, in the US there is an entire technical society with its own journal dedicated to human factors. While there is no society dedicated to human reliability, many technical societies have working groups or standardisation committees dedicated to this field. Even national and international bodies such as the Nuclear Regulatory Commission in the US, and the International Atomic Energy Agency, have endeavoured to establish standards of practice or guidance documents to suggest correct practice related to human reliability analysis. There exists an even larger body of literature, theoretical, experimental and clinical, in the psychological field. However, most of it is related to the performance capabilities of human beings with respect to their mechanical abilities or requirements (range of vision, reach, height, temperature range requirements, lighting requirements, etc.). While there are handbooks filled with these former types of performance requirements and capabilities, the technological basis for all human factors and human reliability technology as it relates to “error-free” performance is very weak indeed. Further, the probability of error-free performance is not the only measure. For some actions, there may be other more important measures.

The determination of which measures should be employed may be industry-specific. So the determination that probability of error-free performance is the proper measure to be used to address human performance in the context of chemical accident prevention, preparedness and response cannot be assumed, but requires investigation and evaluation. In cases where error-free performance is the correct measure, it would be useful to know whether there is support in the technical literature to provide a basis for models which would allow analysts to predict its probability.

In some cases, systems are error-tolerant; that is, they will allow the operator to perform a number of erroneous actions as long as the correct course of action is enacted prior to the point at which recovery is no longer possible and an accident becomes inevitable. It would be interesting to identify the types of current chemical process industry systems which are error-tolerant, and those which are not, and to determine whether those which are not can be made error-tolerant and how this could be accomplished.

The technical research base and models discussed earlier may or may not address error-free performance applicable to error-tolerant systems. If not, it would be helpful to know what research is available to address the probability of human error in these systems.

At some point in the initiation progression, the operator’s performance must be error-free in order to mitigate or prevent an accident. Some discussion is needed to determine whether models which address error-free and error-tolerant situations should ever be combined.

In some cases, the results of errors remain in the system with their impact delayed until other events occur. In other cases, the result of an error is the immediate initiation of an accident scenario. These two different cases might raise different human performance issues, which in turn may impact the evaluation of the error probability.

While there is certainly variation due to the particular scenario being addressed, different systems have different “time constants” or characteristic time frames within which action normally has to be taken to prevent disaster. The time constant for the aircraft and space industry is of the order of seconds, and for the nuclear industry it is of the order of tens of minutes. Perhaps a characteristic time constant can be identified for the chemical process industry as a whole, or for various elements of the industry. This would permit an evaluation to be made of the effect of this time constant on the relationship between the time available for action and the probability of correct action being taken. It would also be interesting to know whether the action required of the operator affects this relationship. Some have suggested that the time available to take an action is an important determinant of the probability of correct action being taken. It has been further suggested that, within certain time constraints, it is the only factor necessary to estimate this probability. It is important to understand whether this is true for the chemical process industry and, if so, when the time available becomes so dominant.

The issue of time constraints raises concerns as to whether there is a time constraint beyond which human action must or should be excluded. This further implies either that psychological and physiological bases can be identified and measured for these constraints, or that these time constraints can be affected by operator selection criteria, training, experience and skill level.

Research in the nuclear power industry, the aerospace industry and academia has suggested a generic model. It is important to determine the applicability of this model to the chemical process industry. If it is applicable, tailoring may be necessary to make it representative of the particular nature of the chemical process industry; if not, perhaps an existing model might be more applicable or the characteristics of such a model might be identified.

Crew Resource Management (CRM)

According to a recently published article in *Scientific American* magazine, in 1978 NASA investigated the causes of US airline accidents since the introduction of turbojet aircraft in the 1950’s. The research showed that more than 70% of airline accidents involved some degree of human error. While this finding was not inconsistent with findings in other industries and therefore might not be considered surprising (although the percentage might be somewhat higher than elsewhere), what was surprising was that most of these errors stemmed from failures in communication, teamwork and decision-making rather than technical shortcomings in design.

These results shocked the industry into paying more attention to failures in interaction and communication, and led to the development of a series of programmes known collectively as “Crew Resource Management” (CRM). Although these programmes primarily focus on the cockpit crew, they also include flight attendants, air traffic controllers and other support staff. The goal of CRM is to get the crew to work as a team so as to reduce errors. Training includes the importance of collaboration to make up for the inherent limitations of human performance, including the impact of stress on the ability to absorb information and make decisions as well as many of the other issues previously mentioned in this paper.

This airline industry programme may or may not be applicable to the chemical process industry given the differences between the two industries. These include: the different actions performed; the aircraft cockpit vs. the process plant control room; the training and background of pilots vs. those of plant operators; the relationship between cockpit captains and their crews, vs. that between senior plant operators and their crews; and the flight operating environment vs. the plant operating environment.

If applicable, consideration should be given to how such a programme could be tailored to meet the specific needs of the chemical process industry.

CRM programmes attempt to assist cockpit crews to interact with their flight management computers as a useful, but not infallible, electronic crew member. It may be possible to relate this to experience with any such programmes tried with the automated operational aids in the chemical process industry, or (if no such experience exists) to determine whether they would be useful to attempt. In CRM programmes, pilots are forced to come face to face with simulated scenarios which are so burdensome that they are placed in error-likely situations unless they disable their automated systems or otherwise limit the input of non-critical information. Discussion of any experience with simulators used in this way in the chemical industry would be enlightening, as would discussion of methods by which such programmes can be implemented without discouraging the operator from the proper use of new automated aids.

Regulatory Systems

Since the operation of chemical process systems can pose a risk to the health and safety of the public, as well as to plant employees, and since the human contribution to this risk has been shown to be significant, federal, state (or department) and local regulatory bodies often play a role in attempting to control this risk. Regulation in a potentially risky business can range from relatively benign self-regulation with occasional auditing, on the one hand, to onerous and burdensome prescriptive restrictions for initial licensing and continued operation. Also, the type of regulation applied is not always consistent across the board. For example, both the commercial air carrier and the commercial nuclear power industries have enviable safety records, but the approach each takes to regulation is very different. While the commercial nuclear power industry might be thought to be more restrictive in its regulations, and so it is on most issues, this is not the case as they apply to individual operations and maintenance personnel, at least in some nations. While both the operators of commercial aircraft and operators of commercial nuclear power plants are initially licensed and are required to take periodic proficiency tests, only air carrier maintenance personnel are always required to be licensed.

It would be helpful to develop a clearer understanding of the regulatory bodies involved in the chemical process industry and the roles they currently play, in an attempt to reduce or control the risk of human error.

Licensing of chemical process facilities operators, maintenance personnel and contract labourers is an important issue to consider. Its appropriateness may hinge upon who should set the requirements for license testing, and whether the government, industry unions or a third party should issue licenses.

Because of experiences in other industries, there is some question as to whether entry requirements outside licensing requirements should be set for licensed positions. Specifically, debate continues as to whether academic degrees or, alternatively, technical schooling or on-the-job training should be required.

With respect to the issue of “fitness for duty” requirements, it should be determined whether this will be evaluated both before and after licensing, how it relates to a balancing of the rights of individual employee operators or other operations personnel against duty requirements, and where the balance line should be drawn.

There may also be fitness for duty conflicts with local cultural and/or medical requirements with respect to use of alcohol or other impairing drug use on and off the job. With respect to these issues, it is important to consider what the government regulatory role should be and whether there should be a role for a transnational regulatory body or involvement of transnational government agencies, since accident effects do not respect international boundaries.

Accident Emergency Response

Despite the best planning and training, accidents can and probably will occur in the future. Once an accident occurs, its consequences may extend beyond the plant site boundary. If and when this happens, response to the accident beyond the local scope of plant management and personnel may be required. When extramural response is involved, it is important that it be co-ordinated and organised so that it is quickly and effectively applied in co-operation with knowledgeable plant staff. However, allowing this unified response to be properly put into effect requires that the response be prepared. This, in turn, implies that the proper procedures have been established, that adequate communications mechanisms and systems are in place, and that adequate response resources have been identified and are available in advance.

Preparation for such events can take different forms. For example, it may be considered appropriate to establish criteria to determine when an internally initiated plant event should be communicated to the external authorities. Or pre-established communications links could be put in place and procedures written governing their implementation.

Co-ordination of response external to the plant with plant management and personnel can be carried out in a variety of ways, but should be addressed before the fact.

There is also a question as to when, if ever, responsibility for emergency response should be transferred from the plant staff to public agencies, and subsequently transferred back to the plant staff when the emergency is resolved.

In some nations and for some industries (notably the commercial nuclear power industry), local and national command centres have been pre-established and provided with significant informational resources and communications links. It would be useful to debate whether some modification of this option would be valid, and affordable, for the chemical process industry.

Finally, consideration should be given to the sort of informational resources and communications links which might be appropriate for accident emergency response at the plant site, for the local region, etc.

Conclusion

In summary, human performance currently is and will likely remain a critical element in chemical process operational safety. Recognition of this undeniable fact suggests that it is in the interest of all those responsible to develop a better understanding of the range and characteristics of human action, and of the global nature of the issues which are likely to guard against poor performance and enhance good performance. Combining basic research into human cognition and behaviour with lessons learned from operating experience would help enhance this understanding. Through conferences and workshops, such as those conducted by the OECD, ideas are expressed and knowledge gaps are identified. However, these findings must be factored into the operational culture. The gaps should be targeted as areas for additional study. Since the responsibility for performance is a shared one, managers, operators, designers and regulators must all play a role in ensuring safe facility operation. Through their combined efforts, the industry will benefit from inherently safe designs whose operation balances the best of human, hardware and software performance in a watchful but not heavy-handed regulatory environment.