SUMMARY

First, this paper gives a short general review on important safety issues in the field of man machine interaction as expressed by important nuclear safety organisations. Then follows a summary discussion on what constitutes a modern Man-Machine Interface (MMI) and what is normally meant with Accident Management and Accident Management strategies. Further, the paper focuses on three major issues in the context of accident management. First, the need for reliable information in accidents and how this can be obtained by additional computer technology. Secondly, the use of procedures is discussed and basic MMI aspects of computer support for procedure presentation are identified followed by a presentation of a new approach on how to computerise procedures. Thirdly, typical information needs for characteristic end-users in accidents, such as the control room operators, technical support staff and plant emergency teams is discussed. Some ideas on how to apply virtual reality technology in accident management is also presented.

1. INTRODUCTION

Many questions have been raised in considering what kind of Man-Machine Interface (MMI) and what kind of decision support to provide to nuclear plant operators, in particular in transients leading up to and during accidents.

Professor Tom B. Sheridan from MIT has in the following apt way characterised the interaction between a human operator and a complex system (Sheridan, 1996): “As systems of all kinds become more and more complex, there is a great reluctance to replace the human operator, since unexpected circumstances may arise which the automatic or computer-based control can not handle. Having a human operator as a final authority provides a sense of comfort, and is more politically acceptable than having no operator. Yet, at times of system failure or other abnormal circumstances the human operator is often overwhelmed. So it seems reasonable to provide the operator with computer-based advice - through the Man-Machine Interface - in a form which integrates the available data, is understandable and provides useful advice on the plant state and the transient progression.”

Many organisations take the MMI question seriously. Nuclear organisations such as the United States Nuclear Regulatory Commission (USNRC), the International Atomic Energy Agency (IAEA), the OECD Nuclear Energy Agency (NEA) as well as the European Commission put much importance on MMI issues. The importance of a well-designed Human-System Interface (HSI) to reliable human performance and nuclear safety is widely acknowledged. Moray and Huey, for the USNRC, (NRC 1988), reported that the errors at TMI were due to a number of factors including a poorly designed CR and inadequate provisions for monitoring the basic safety parameters of plant functioning. In an IAEA Safety Report, (IAEA 1997), it is stated in the introduction: ”The human-machine interaction problems are complex. In many applications, the role of the human operators is often neglected in design and the human functions are defined by default, governed by the limitations and gaps of hardware and software. It is questioned if the role defined by implication for the operator can be effectively and reliably performed”. OECD NEA has
established a Senior Group of Experts on Safety Research (SESAR). In a NEA Report, (NEA 1995), the major themes for further research are identified as:
- Characterising and assessing the performance of individuals, teams and organisations
- Man-machine interfaces and communications in the control room and other plant areas
- Selection and training of staff
- Signal validation and condition monitoring methods for severe accident situations
- Development of operator support systems using advanced data processing and MMIs

The European Commission in its 5th Framework programme 1998-02, in the key action “Nuclear Fission”, has a strong focus on reactor safety, advanced nuclear reactor design and safety. To achieve the new Community research objectives of sustainability and competitiveness, an all-embracing approach is proposed in the area of nuclear safety. This means to improve the defence-in-depth strategy, including not only the new safety systems, but also more efficient MMIs (EC 1999). This became one of the subjects of the research area of the EC key action “Nuclear Fission”, called “Operational Safety of Existing Installations”.

Considering the changing role of the operator because of higher level of automation both in the nuclear and the non-nuclear industry, the tendency is that the non-nuclear industry is going further than the nuclear in terms of advanced solutions. Accordingly, the operator role in the non-nuclear industry is becoming more ‘operation management oriented’ than the nuclear operators who can be characterised more as ‘manual operation and monitoring’.

2. MAN-MACHINE INTERFACE

The importance of a well-designed MMI to reliable human performance and Nuclear Power Plant (NPP) safety is widely acknowledged as documented above. In response to such requirements the USNRC, issued an extensive Human-System Interface design review guideline called NUREG-0700 (NRC, 1996). This document provides a thorough discussion on what constitutes the MMI or as the Americans call it - HSI – the Human System Interface - as well as guidelines for how to perform human factors engineering reviews of the HSI. A summary of various areas of MMIs both in advanced and conventional control rooms can be found in Table 1, and examples found on the next page. Other references that should be mentioned in this context are related to the work performed within the International Organisation for Standardisation (ISO). Examples are: (ISO 11064, ISO 9241 and ISO 9355).

<table>
<thead>
<tr>
<th>Different Areas of MMI</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Displays</td>
<td>Visual displays, (e.g., mimic displays, trend graphs; format elements)</td>
</tr>
<tr>
<td>User-System Interaction</td>
<td>Interaction between the user and the MMI, (e.g., dialogue formats, navigation, display controls, entering information, system messages)</td>
</tr>
<tr>
<td>Process Control and Input Devices</td>
<td>Information entry, dialogue types, display control, information manipulation and system response times</td>
</tr>
<tr>
<td>Alarms</td>
<td>Alarm system design implementation, (e.g., alarm conditions, choice of set-points, alarm processing, display of alarm information)</td>
</tr>
<tr>
<td>Analysis and Decision Support Aids</td>
<td>Aids for overall situation analysis, prediction and decision making.</td>
</tr>
<tr>
<td>Inter-Personnel Communication</td>
<td>Speech and computer-mediated communication</td>
</tr>
<tr>
<td>Workplace Design</td>
<td>Design of consoles, workstations, instrument panels, furnishings, and general CR arrangements as well as the CR environment</td>
</tr>
<tr>
<td>Local Control Stations (LCS)</td>
<td>Labelling, LCS indicators, LCS controls, communications with personnel outside LCS.</td>
</tr>
</tbody>
</table>

Table 1. Different MMI areas and content from NUREG-0700, Rev.1.
Examples of MMI-types, user interaction objects, display design principles and workplace design from development work at the OECD Halden Reactor project.
3. ACCIDENT MANAGEMENT

The concepts of accident management and accident management strategies are discussed in the following paragraphs.

Accident management

Accident management can be defined as those actions that can be taken by the plant staff to prevent accidents or mitigate their consequences. Its objective is to further reduce the risk of plant damage and minimise radioactive releases to the environment (NEA, 1992).

Accident management strategies

An overall structure, which clearly delineates responsibilities and any transfer of responsibilities during the development of an accident, is the essential starting point. In practice, a combination of approaches may prove to be most effective since the needs of the control room operator, support staff, and emergency management teams may not necessarily be best met by the same approach.

So several elements are needed for successful accident management. The ones currently implemented by most utilities consist of procedures, organisation and training, co-ordinated with emergency planning. While the form these elements take may differ considerably from one plant to the next, together they must form a coherent, co-ordinated whole at each plant.

Procedures

Devising procedures for accident management actions means that the directions the operating staff receives are very specific and in a familiar format. On the negative side, such an approach could lead to inappropriate actions if a situation occurred which was not foreseen during procedure development. Procedures, which are symptom oriented, can address this concern to some degree, but such procedures may be difficult to devise given the variety and, in some cases the paucity, of detectable symptoms produced by severe accidents.

Development of a guidance document is another alternative. This type of guidance might identify equipment, water supplies, and power sources needed to restore safety functions, but without providing the details of implementation. Such a guidance document allows consideration of the pros and cons of an action given the plant conditions as they are known. This approach would lead to a slower response than one that follows an explicit procedure and would require the availability of more independent technical expertise.

Computational aids for accident management

During an accident, plant operators and technical support staff need access to plant status, and monitor plant response to the actions taken. They also need to infer likely plant response to possible mitigative actions as well as the near-term plant behaviour in the absence of mitigative actions. These are very challenging tasks since a nuclear plant will be in an accident state only as a result of unexpected multiple failures.

Simple computational tools as proposed by EPRI in (EPRI, 1992; EPRI, 1993) and/or step-by-step instructions, which can be performed by means of hand-held calculators or palmtop-computers, can be used to estimate plant responses.

Comprehensive computer-based support systems for accident management actions aim to assist the plant operators and other technical support staff in implementing accident management strategies on a continuous and automatic basis. These systems can be used to monitor the current status of the plant and to project the progression of key phenomenological events. Several such systems have been developed for example at the Halden project (CAMS, 1997) and some are commercially available, for example (MARS, 1993) and (ADAM, 1999).

One main goal of a plant site emergency team is to provide protection to the public from accidental radiological releases. To help achieve such a goal on-line monitoring systems have been developed and the main functions are to provide reliable plant status, radiological and environmental data. These data are used by decision-makers to determine the best
possible public protective action recommendations consistent with existing and predicted risk. An example is the Accident Monitoring system for the US state of Illinois (Illinois, 1995) another is the Norwegian Emergency Management system (MEMBRAIN, 1994) and the Emergency Response Support System for Japan (ERSS, 1993).

4. RELIABLE INFORMATION DURING ACCIDENTS

Nuclear power plant personnel currently have the capability to manage a broad range of accidents. Accidents will occur only if there are multiple failures of safety related equipment, serious human errors, or some combinations of these two conditions. Successful management of this complex accident behaviour requires that plant personnel diagnose the occurrence of an accident, determine the extent of challenge to plant safety, monitor the performance of automatic systems, select strategies to prevent or mitigate the safety challenge, implement strategies, and monitor their effectiveness. The capability of the staff to effectively carry out these actions is directly influenced by the availability of timely and accurate plant status information which the plant instrumentation is relied upon to supply.

AI methods, mainly Neural Networks and Fuzzy Logic techniques, have gained considerable attention in the last few years, due to their ability to deal with uncertainties and the non-linearities usually embedded in real processes, especially in abnormal conditions.

An example is the PEANO data validation system (PEANO, 1999), which is based on neuro-fuzzy techniques. In PEANO the signal validation process is divided in 2 stages:
- A fuzzy pattern recognition where all the possible process operation or accident states are identified and classified in “Fuzzy clusters”
- A Neural Network (ANN) bank, where each ANN is connected to only one operational state (cluster). Each ANN is specialised only in one of the many possible plant states.

A special feature of this architecture is that unknown process states would promptly be recognised as an “unknown” scenario. This architecture has been developed at the Halden Project and has been tested successfully both in normal and accident conditions. It is now operating at the Halden Reactor. In the PEANO MMI the user can select between a number of plant variables to check current values, trends, deviations and reliability. Prompted by an alarm, the operator can see signal deviation, estimated correct value and reliability.

5. COMPUTERISED PROCEDURES

Procedures have changed a lot since the TMI accident, most notably is the introduction of symptom-based emergency operation procedures (EOPs). They have changed mainly to reflect changes in control room technology and automation, but the structure has remained the same, as has the their format, i.e. printed documents or handbooks.

<table>
<thead>
<tr>
<th>Aspects</th>
<th>Level 4 development</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigation</td>
<td>Intelligent access to procedure</td>
</tr>
<tr>
<td>Formatting</td>
<td>Enhancing the logical structure of procedure</td>
</tr>
<tr>
<td>Progress Monitoring</td>
<td>Automatic progress monitoring</td>
</tr>
<tr>
<td>Help and Explanation facilities</td>
<td>Context and User sensitive (model based) help</td>
</tr>
<tr>
<td>Process linking</td>
<td>Plant variable limit values and actual values</td>
</tr>
<tr>
<td></td>
<td>Access to historical trends and predictions</td>
</tr>
<tr>
<td>Procedure adaptation</td>
<td>Procedure adapts to process and operator conditions</td>
</tr>
</tbody>
</table>

Table 2. Basic MMI aspects of computer support for procedure presentation

In their study Green and Hollnagel (Green, 1997) analysed the basic MMI aspects of computer support for procedure presentation and identified the following six aspects, with four levels of development, see the highest Level 4 in Table 2.

The recommendations from the Green et.al study were the following:
1. Movements through procedures should be based on display pages, or segments, rather than being continuous. This makes it easier for the operator to establish where he is (orientation, navigation). Similarly, displays should not be larger than the physical screen. If larger, scrolling is required, and this is an unnecessary task that should be avoided.

2. Formatting should use well-defined fields in fixed positions. It is important that operators can recognise a procedure page and that they do not have to search for information.

3. Windows and panes should avoid overlapping, because this may block important information, or cause operators to lose orientation.

4. Multiple substeps of a procedure step should be presented with each item separately. Each item can then be acknowledged when performed. This provides a suitable basis for progress monitoring, additional explanations etc.

5. The required interaction (navigation) should be minimised. The structure should be as simple as possible from the user's point of view.

A notably characteristic of early versions of computerised procedure systems is that it has required a reformulation and re-structuring of the procedure before taking them into use. A fixed set of steps and instructions and a fixed procedure structure made the computerised version (in most cases) very different from the original hard copy version. Work at the Halden Project is on-going to remedy this. In COPMA-III, Nilsen et al. (COPMA, 1999) aims to enhance old procedures without having to change much of their original layout.

In COPMA-III one can insert into the old procedure text tags that describes the “meaning” of the various textual elements in the procedure. These tags can be made invisible to the person executing the procedure, but the computer is able to inspect the tags and give appropriate assistance in carrying out the procedure. Also, by means of small procedural elements (micro-elements), it is possible to configure the system to fit the set of instructions and the procedure structure that is being used by the old hard copy procedure system. An example procedure MMI for a self-explanatory example procedure is shown in Figure 1.

6. PREDICTIVE SIMULATION

The main task of a predictive simulator is to inform the staff about what will happen in the near future. Another task is to allow the operator to test mitigation strategies before they are actually carried out on the plant. To be of any use, the speed of such a predictive simulator must be faster than real time, actually much faster (~100 times). This will of course depend on the way the plant modelling is done and the performance of computer hardware.

Two Swedish BWR’s have been modelled in the CAMS project at the Halden Project and results from the use of this system in a safety exercise is reported in (SKI, 1995).
general, the whole plant is not modelled, much of the turbine-part is omitted and simplified models were used in many cases. The reason for this approach is of course that detailed models leads to more calculations and less speed. The modelling was performed with the Finnish APROS code (APROS, 1997). The simulator can be used in normal transients as well as in accident conditions up to cladding temperatures of 900 degrees C. A severe accident extension of this approach was performed successfully by a Spanish team using the MAAP code as basis (Iberdrola and Union Fenosa, 1999).

7. INFORMATION NEEDS IN ACCIDENTS

In case of an accident, or an event that may develop into an accident, the plant personnel must perform various tasks before they can start actions to counteract the incident:

- **Identification of the plant state**, this may typically be a diagnostic task to find the cause of the problem and validate the state of critical parameters.
- **Assessment of the future development of the accident**, this involves prediction of future states and behaviour of the plant.
- **Planning of accident mitigation strategies**, this is where various alternatives are tested.

The end-users are control room operators, technical support staff, emergency staff and other utility and authority staff coming on scene. They will have varying needs for information, but basically they will ask:

- Is the available information correct?
- What are the most important things going on in the plant just now?
- Which subsystems are in order and which are not?
- How far is the present state from the relevant danger limits?
- How to get information about physical quantities not directly measurable?
- What will happen if I do nothing?
- What will happen if I carry out this plan?
- What is the best strategy in the present situation?

The MMI shall display information in such a way that one easily gets a mental picture of what is going on in the plant. This information may be measured physical quantities like pressures, temperatures, flows, or valve positions. But it may also be quantities derived from the measured ones. Actually, many interesting quantities cannot be measured. The temperature in the middle of a fuel element cannot be measured. But it can be calculated without too much difficulty.

Physicists and engineers use concepts like energy, enthalpy, entropy, eigenvalues, poles, stability diagrams etc., to facilitate their thinking about power plants. Would any of these concepts be useful for the plant staff in an accident state? One should try to use the imagination to invent such derived quantities and assess their usefulness for the operators and the technical support people. Here are some quantities, which we think will be informative:

- Flow and build-up or depletion of mass (water and steam).
- Flow and build-up or depletion of energy.
- Leakage amount and rate.
- The temperature profile from the centre of a fuel element to the outside of the cladding.
- Water inventory of the containment.

**Plant Layout and Administrative Information**

In many ways the support systems of today are oriented towards system functions. In a possible accident, but also in normal operating states, there is also a need for information based on layout of the plant. For example, a fire incident primarily occurs in a room, not in a system, the same applies to a radioactive leakage. Both operators and rescue staff will need information presented at least on layout diagrams.

Information of location of fire alarms, radioactive leakage detectors and personnel movements can be very helpful to decision makers to understand what has happened in a
confusing situation. Information can be provided by combing information from several databases, such as the process computer, fire alarm system, radiation monitoring database, chemistry database, the administrative data base, work permit data base etc. Data must be made available through the plant network information in order to achieve this.

8. VIRTUAL REALITY (VR) TECHNIQUES IN ACCIDENT MANAGEMENT

Virtual Reality has been defined as “A computer system used to create an artificial world in which the user has the impression of being in that world and with the ability to navigate through the world and manipulate objects in the world.”

VR techniques can be applied in Accident Management as a tool for improving communication between the management and the rescue team in emergency situations. A VR model of the emergency scene can be visualised by a projector and a large screen for easy audit and inspection for a large number of people simultaneously. The VR model can easily be changed to reflect the current emergency situation. Another possibility is to connect the VR model to a simulator or prediction system. VR technology can be used as a tool for coordinating resources and ensuring open and effective communication channels within the operation team. Members of the rescue team not familiar with the scene of the accident can be briefed by using the VR model prior to entering the area. The Halden project is currently developing VR software for route planning of work tasks in high-risk environments (VR, 1999). This route planning can be combined with other data such as radiation maps and individual worker radiation doses. Work-task reports and/or maps can be generated for use by the rescue teams containing 3D illustrations of the problem areas combined with textual information. The routes can be visualised as a replay of the work task using virtual manikins or as way-points or vectors, see Figure 2.

9. CONCLUSIONS

Computers are better than humans, and Humans are better than Computers

It is firmly believed that computers provide a useful tool for operators, technical support staff and emergency teams in an accident situation. This applies to the task of obtaining reliable information, to follow procedures, to identify plant states, to predict the future progression of the accident and to plan mitigative actions. Of course, both state estimates and predictions will only be approximate. But the alternative is essentially more or less intelligent guesswork. We are confident that at least some of the detailed phenomena that take place in a nuclear power plant in an accident situation are more accessible to computation than to common-sense evaluation.
Humans are however better than computers in keeping track of the broad lines and completely superior to computers in handling the unexpected. Computers should be used for what they are really good at: transforming information from one form into another. In our minds, this property is utilised in transforming what can be easily measured into what can be easily understood.

10. REFERENCES


IAEA, 1997 “Safety Issues for Advanced Protection, Control and Human-Machine Interface Systems in Operating Nuclear Power Plants”

ISO 11064: ‘Ergonomic Design of Control Centres’ (under development)

ISO 9241: ‘Ergonomic Requirements for Office Work with Visual Display Terminals’

ISO 9355: ‘Ergonomic Requirements for the Design of Displays and Control Actuators’

IEC 964: ‘Design for Control Rooms of Nuclear Power Plants’


MEMBRAIN, 1994 E. Stokke “Membrain – the Norwegian Emergency Management System” Seminar on Disaster management, September 1994, Constanta, Romania


