SAFETY AND RELIABILITY SOCIETY SYMPOSIUM 1988

"HUMAN FACTORS AND DECISION MAKING,
THEIR INFLUENCE ON SAFETY AND RELIABILITY"

Altrincham, Manchester, UK, 19-20 OCTOBER 1988

ADDRESSING HUMAN FACTORS ISSUES IN THE SAFE DESIGN AND OPERATION OF COMPUTER CONTROLLED PROCESS SYSTEMS

LINDA J. BELLAMY and TIM A. W. GEYER
Technica Ltd, Lynton House, 7/12 Tavistock Square, London WC1H 9LT

ABSTRACT

Incidents that occur in computer controlled process systems would appear to involve human error at all stages from design through to operation. Some examples are given. To overcome the sources of error is problematic because guidelines and analytic methods specifically relating to human factors in computerised process control do not exist.

We have attempted to address some of these problems by highlighting areas that could be considered in providing design guidance and by emphasising the need for a design review methodology.

INTRODUCTION

Work has been carried out by Technica for the Dutch authorities to develop a methodology to review the design, operation and modification of computer controlled process systems. As part of this work, human factors issues were considered, particularly those aspects relating to safety.

As far as we know, there are no accepted well defined design standards or methodologies for dealing specifically with the human component in computerised process control systems. The recent PES (Programmable Electronic Systems) Guidelines (HSE, 1987) identifies the importance of the operator's role, the man-machine interface, supervision, training and procedures but hardly goes into detail on these issues, and neither does it devote a special section to them. The Guide to Reducing Human Error in Process Operation (SRD, 1985), while addressing human factors issues explicitly, provides a list of guidance principles that are short, simple and concise.

This is not meant to be a criticism. Rather, it emphasises the fact that, for complex control systems, detailed point by point instruction on all aspects of design and operation would be difficult to achieve. Marshall et al (1987), in writing about guidelines for the design of the user

interface for complex computing systems, say that:

> "... user-interface design guidelines cannot provide an automatic solution to the design problem. They do not tell the designer how to do exactly the right thing and they do not tell him or her exactly when to do it."

They go on to suggest that, in order to make genuinely useful statements guidelines must be context free. Guidelines are often based on informed opinion rather than on hard data. They should therefore be viewed as an informal collection of suggestions, rather than as a distilled science. Designers are likely to have to make some choices of their own and be prepared to test their work empirically.

In addressing the human factors issues involved in the safe design of computer controlled process systems, it is in this spirit that this paper is written.

To put the human factor into context, a summary of an analysis of 17 accidents is first given. A simple information processing model is used to illustrate human factors thinking in carrying out such an analysis. This model then provides a basis for consideration of the kinds of human deviations that could be included in a HAZOP. Before this, a simple set of design principles for computer controlled process systems are presented.

INCIDENTS IN COMPUTER CONTROLLED SYSTEMS

Descriptions of 17 incidents which had occurred in computer controlled systems were reviewed to identify broad classes of failures. These failures led mainly to small and medium sized releases, in one case plant damage, and in another a fireball. Table 1 shows a summary checklist indicating the number of failures in each category (hardware, software, human etc.). For any particular incident it should be noted that the failures are not independent eg. some failures led to others.

From this summary it can be seen that human errors during operations were associated with 59% of the incidents. Errors were mainly due to inadequate, insufficient or incorrect information supplied to the operators (59% of incidents) and a failure to correctly follow procedures (47%). Human errors in design were involved in 29% of incidents. Hardware and software failures were less prominent. Interestingly enough, most of the causes of failure in these computer controlled plants could equally well have occurred in conventionally controlled systems.

Figures 1 & 2 illustrate how the failures can arise in the man-machine system. The model shows the basic information processing operations of the human operator. Superimposed on this are the stages leading up to an accident. These are described after introducing the model components.

The model shows that the operator perceives a situation based on the information displays available. It should be stressed that the operator will act on his perception of a situation which may not always reflect the real situation. Decision and response selection is based on information

perceived and information stored in memory. **Long term memory** refers to stored knowledge gained from experience, training etc. which influences the way we perceive new experiences. **Working memory** is a short term store for data momentarily required for a particular task (eg. remembering a telephone number long enough to dial it). This short term storage mechanism has a limited capacity. Following decision and response selection, **execution of a response** may occur.

Perception, decision making, response selection and response execution all require **attention resources.** These resources are limited and can be exceeded under adverse conditions (eg.high stress). When responses are well learned there is less need for such resources (eg. consider the development of car driving skills).

Response execution usually involves acting on some controls to affect the process, which may cause a change in displays. This forms a feedback loop whereby an operator gains information about the effects of his control actions. In a highly automated system, where the operator acts principally as a monitor and only steps in when the automatics fail, the majority of actions may involve searching displays, paging through the data base, logging values etc.

Failures can occur at any point in the model. In the examples shown on the model, the course of events can be seen by working through the numbered comments in order.

In the incident shown in Figure 1 the bottom discharge valve of a reactor was open when a batch job was started. The operator thought the valve was closed because this was the status displayed. The result was a release of more than 15 tons of vinyl chloride gas.

Figure 2 shows how problems can arise when the operator does not have all the required information available in parallel. In this incident the operator focussed all his attention on the furnace such that he missed what was happening near the scrubber. The fact that the alarm display was a scrolling screen showing only the last 12 alarms resulted in the low level alarm for the cooling system being missed. For this event where lots of alarms were being triggered, the operator lost control of exactly what went wrong and where. As a result, serious damage to part of the plant occurred due to exposure to extremely high temperatures.

Table 2 provides a more detailed breakdown of the causes of the 17 accidents. As can be seen, poor information provision, whether incorrect, hidden, or not available derives from a number of sources. It is likely in some cases that the quality of procedures, supervision and checking were insufficient to enable errors to be identified and recovered (eg. in installation and maintenance). On the other hand, over reliance on the computer when carrying out procedures could reflect inadequate understanding by operators of the functions performed by the computer and how these are carried out.

TABLE 1

Checklist used to identify broad classes of failures for 17 computerised process control system incidents (individual incidents may be associated with more than one failure category)

FAILURE CATEGORY		NUMBER OF INCIDENTS	% OF INCIDENTS
HARDWARE	Computer Hardware	3	18
	Connection Hardware		
	- Electronic	0	0
	- Pneumatic	0	0
	- Electrical	1	6
	Protective System Hardware	0	0
	Equipment Hardware	5	29
SOFTWARE	System Software (Manufacturer's Shell)	1	6
	Site software implementation (i.e. Software written for the process plant and installed during and after implementation)	2	12
HUMAN	Error Context		
	- Design	5	29
	- Installation	2	12
	- Commissioning/Testing	1	6
	- Operating	10	59
	- Maintenance	2	12
	Error Type		
	- Failure to follow procedure (correctly)	8	47
	- Recognition failure, given adequate supply of information	2	12
	- Error due to inadequate/insufficient/incorrect information supplied to person(s) involved	10	59

TABLE 2
Breakdown of causes of the 17 incidents

HUMAN AND SOFTWARE ERRORS	**INCIDENT NUMBER CODE**
Interface does not display actual plant status	1, 6, 8, 16
Installation error leads to incorrect information	3, 8
Alarm set incorrectly	4
No alarm (maintenance error)	4, 5
No alarm (design)	4, 5
Operator misses information due to overload	2, 13, 15, 17
No independent means of cross checking provided	1, 3, 6, 16
Operator fails to cross check	8
Trip disabled/manual override	1, 8, 11
Over-reliance on computer	9, 11, 14, (15)
Inadequate knowledge	(3), 11
Failure to update operators' information	12, 17
Incorrect control signal (maintenance) error	10
Design error: Plant	4, 5, 8, 17
Design error: Computer control system	7
Software error	7, 9
HARDWARE FAILURES	
Equipment hardware	2, 5, 13, 14, 15
Computer hardware	7, (11), 16
Connection hardware (electrical)	6

(Note: Incident numbers in parenthesis indicates that there was not enough information to allocate to the failure category with certainty).

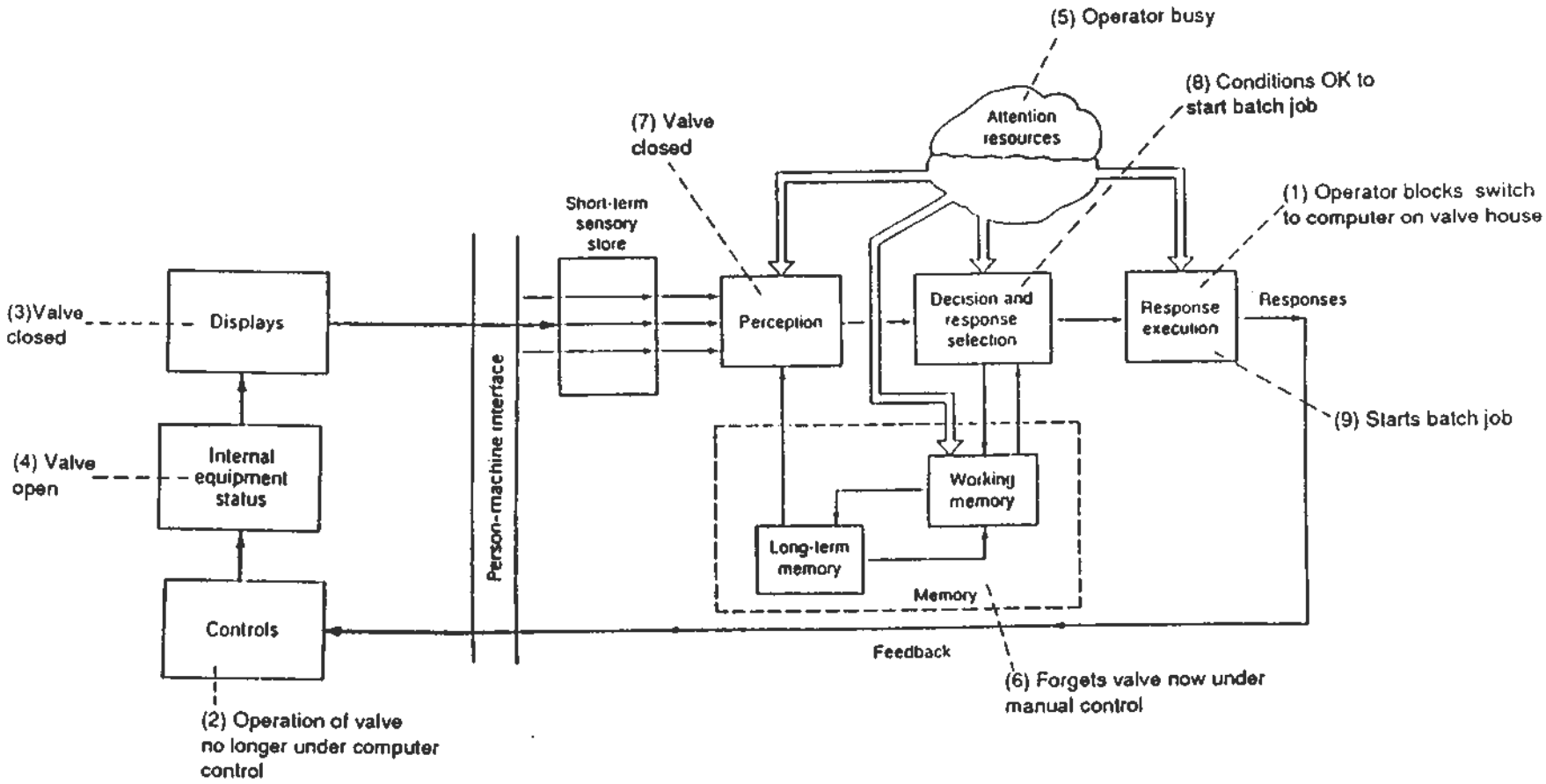

Figure 1. A model of man as an information processor in a man - machine system (adapted from Meister, 1971 and Wickens, 1984) showing analysis of incident 1

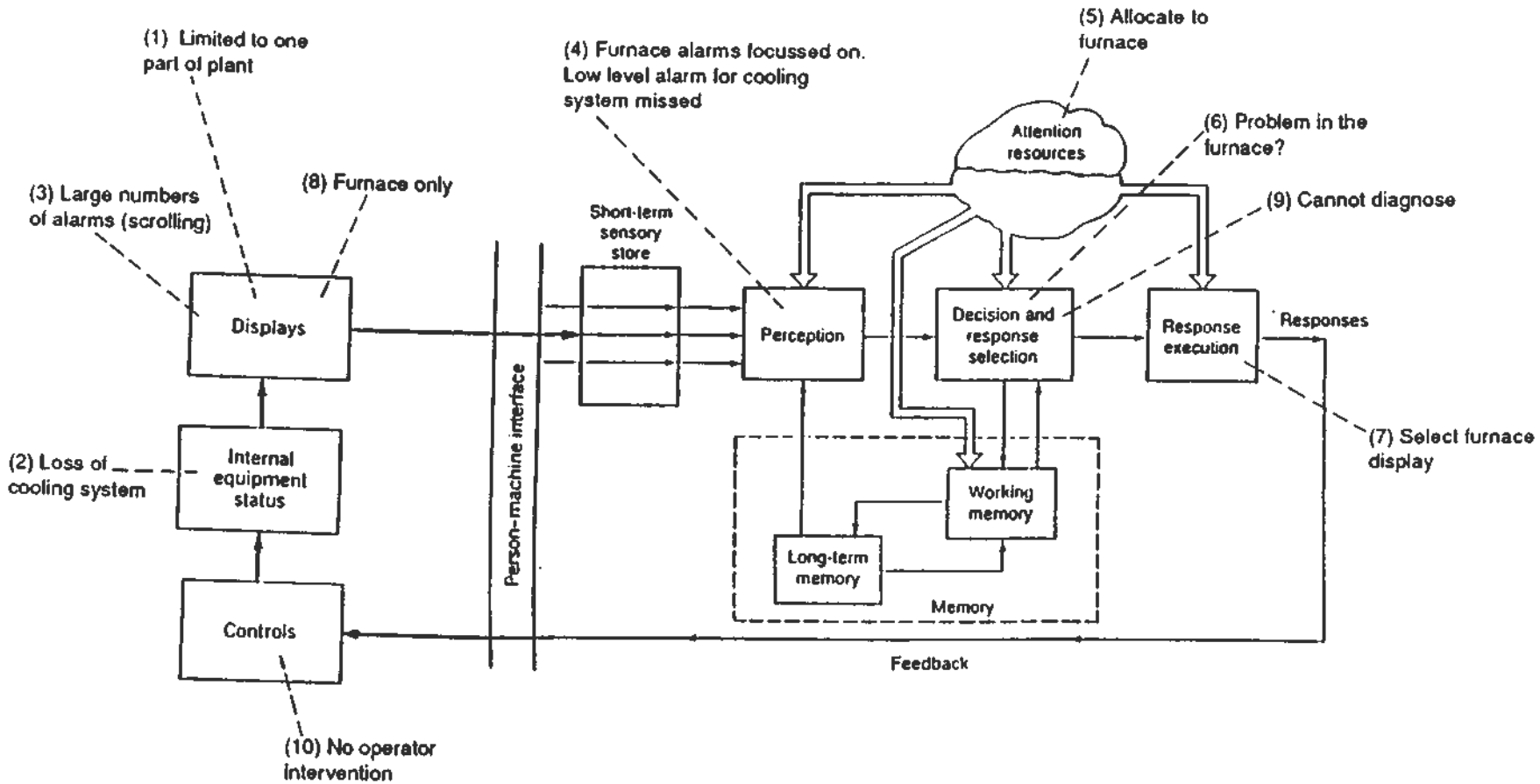

Figure 2. A model of man as an information processor in a man - machine system (adapted from Meister, 1971 and Wickens, 1984) showing analysis of incident 2

DESIGN GUIDANCE FOR THE MAN-MACHINE INTERFACE

Human-Computer Collaboration

Bainbridge (1983) has summarised some of the major problems that automation brings to the design of the operator's task, interface with the system, training and procedures. Bailey (1982) discusses some of the problems of allocation of function between the human and the machine. If one extracts the major issues applicable to computer systems from these two sources, a set of general recommendations can be made:

1. Operators should not be left with an incoherent set of functions that the designer cannot think how to automate. Operators need proper support for carrying out tasks after automation and this means thinking about how the operator and computer collaborate in carrying out the various control functions.

2. When the role of operators is mainly one of monitoring, it is essential to maintain the necessary operator skills, knowledge and mental model of the system. This can be achieved in two ways:

   (i) Allowing operators to take over from automatic operations to get "hands on" experience.
   (ii) Use of high fidelity simulators where realistic failure scenarios can be used to train operators to adopt good general problem solving strategies (eg. for low probability events) rather than specific responses such that these strategies can be used in cases of unanticipated failures.

3. It is essential that operators are aware of exactly which parts of the system are under computer control and which are in manual mode, especially in high periods of activity such as an emergency. If the operator needs to follow what the computer is doing (eg. in an automatic shutdown) it may be necessary to think about presenting this information in new ways that are compatible with his skills eg. slowing down the display of automatic events that are too fast for him to follow. If this is not possible, then one cannot allocate this role to him.

4. It is important that failures are made clear to the operators in time for them to both think out what to do as well as take corrective action. The control system should not disguise the failures to limit this thinking time. The need for operators to think out the effects of possible actions must be considered in design when selecting amongst alternative solutions.

5. Clear criteria need to be provided for the operators to indicate when there is a necessity to take over from the automatic operations as operators may not be able to work this out for themselves.

6. The relative merits of human and computer control should be taken into account. Human operators have distinct strengths above that of machines for certain tasks, e.g. adapting to a novel set of conditions, pattern recognition, etc., whereas machines are better than humans at others e.g. fast responses.

Principles of Interface Design

Interface design principles were developed for the specific problems involved in computer controlled process systems. The principles refer essentially to operator monitoring and control tasks.

There were 5 main principles used:

[A] Provide the operator only with information that he needs and none he does not need.

[B] All the information relating to a particular task should, as far as possible, be grouped together in one place.

[C] Operator's experience affects the way they read a display or operate a control, so their expectations should not be violated as they move from one physical location (or VDU page) to another.

[D] The design of the interface should be compatible with the operator's limitations and capacities as an information processor.

[E] Manning should meet resource requirements. Personnel should not be predominantly either overstressed or bored.

The principles were broken down into a number of specific recommendations. An example is shown below for Principle B.

Principle [B] All the information relating to a particular task should, as far as possible, be grouped together in one place.

[B1] Determine information requirements for tasks by carrying out task analyses.

[B2] Controls and displays related by action and effect (feedback) should be located together as far as possible.

[B2.1] All the effects of a keystroke command on the process should be simultaneously observable on the operator's displays. If the process response time is slow some feedback must still be given that the action has been initiated.

[B2.2] If more than one person must work on the same part of the system, all the relevant information should be simultaneously available to a person coordinating the task. (This includes the coordination of control room and maintenance tasks etc.)

[B3] As far as possible, supply all the necessary information simultaneously (i.e. in parallel rather than sequentially) that is needed for a diagnosis or a control decision.

[B3.1] The operator should not have to page through the displays to collect together all the information relating to a particular failure

[B3.1.1] Sufficient VDUs should be available for simultaneous display of the required information if it is likely to appear on different display pages.

[B3.1.2] As far as possible within physical and ergonomic constraints, all the information needed for diagnosis of one failure should appear together on one display page. Therefore all the variables affecting a controlled state should be, as far as possible, displayed together.

[B3.2] The minimum number of VDUs will partly be determined by the number of unrelated failures that could occur simultaneously:

[B3.2.1] Never use only one VDU per workstation for monitoring and control tasks.

[B3.2.2] Additional VDUs may be needed for dedicated displays (e.g. alarms).

[B3.3] Certain display divisions are acceptable. These are cases where the cause and effect relationship between plant/process variables is simple. Different display pages should not cut across interacting variables. This point relates not only to the division of displays at one operator station, but also division of displays between operator stations.

[B3.4] The operator will need to be able to see cause and effect relationships, time lags and rates of change in the process.

[B4] Minimise uncertainty.

[B4.1] Provide an overview display that will satisfy the operator's need to keep a summary check on the whole of the system for which he is responsible. (This could be a wall mounted display.)

[B4.1.1] Provide alarm overviews that are permanently on display.

[B5] Avoid operators having to move around too much to different locations to collect or transmit information.

[B5.1] Consider using flexible as well as fixed communication equipment.

[B5.1.1] Communication systems for transfer of current information should not require operators to leave their consoles.

[B5.2] Consider conference facilities if communication needs exceed one-to-one for coordinated tasks.

[B5.3] It should be possible to display any information from the plant data base on any VDU.

[B6] Centralise important information.

[B6.1] Consider using a dedicated alarm VDU at operator workstations.

[B6.2] Consider providing a summary of important information for supervisors to allow prioritising of actions.

[B7] Locate related items such that they are easy to associate.

[B7.1] Locate alarm displays close to (or on) other displays with which they are associated.

[B7.2] Group alarm summaries in a meaningful way (i.e. according to sequence, priority, function etc.)

[B7.3] Locate acknowledgement devices such that alarms cannot be acknowledged without being identified first.

[B8] Avoid two operators (or an operator and supervisor) being able to simultaneously affect the same part of a process from different VDU/keyboard locations

[B8.1] If [B8] is unavoidable, information on each operator's actions will have to be provided and supervised in these situations, imposing an additional monitoring load. (If there are two unrelated failures this may not be a problem).

We do not consider that this is necessarily a comprehensive list. However, we have endeavoured to cover all the major areas which are highlighted by previous accidents, by ergonomics analysis of the problem areas (e.g. Bainbridge 1983) and current ergonomics practice.

HUMAN FACTORS HAZOP REVIEW OF COMPUTER CONTROLLED PROCESS SYSTEMS

Many incidents arise in non-safety critical areas of the plant, as was found in the 17 that were examined here. For this reason guidelines which only address critical safety systems are insufficient where the design review needs also to cover incidents with the potential to cause damage or serious environmental effects. We have already shown that human error plays a large part in such cases.

We consider that extending hazard and operability studies (HAZOP) to include human factors could go some way towards dealing with problems in design which could lead to human errors with consequences relevant to plant safety. HAZOP is a method for checking a design by applying a limited set of guidewords and variables to examine the suitability of the design to respond to a whole range of deviations.

Deviations are derived by combining a set of guidewords (eg. NO, WRONG etc.) with a set of variables (eg. SIGNAL, ACTION etc.) and these deviations are then applied to some element of the design in the form of questions (eg. "What happens if there is no signal when there should be").

By adapting the information processing model (Figure 1 and 2) to this format we have derived the following:

GUIDEWORDS	VARIABLES
MORE	INFORMATION
LESS	ACTION
NO	
WRONG	

The variable INFORMATION applies to information available from displays, procedures, previous training, experience, communications and any other source which an operator may use. The variable ACTION refers to the operator response. Errors in ACTION may be in terms of incorrect selection or incorrect execution of a response.

A set of specific deviations can then be provided for each of the 8 deviation categories. An example for NO ACTION is given below:

NO ACTION

This deviation occurs when the operator fails to act when there is a demand to do so.

Example Causes

Control cannot be accessed
Error recovery not possible
Necessity for action not perceived
No information to act upon
Action not possible
Assume computer control of operator function
No operator present
Operator distracted
Omit procedural step(s)
Communication failure
Action too late
Assume other person has acted
Insufficient time to complete
Fail to restore to automatic control
No supervision/checking/testing

We propose to test out this method in the future using details of a site specific interface design, procedures, and control philosophy documentation.

CONCLUSIONS

There is a wealth of human factors knowledge that could be put together in a simplified form to enable design engineers to incorporate human factors early in the design process when changes can be made at relatively little cost.

It would be useful if guidance principles and review methods could be standardised to enable them to be applied with confidence. To do this would require collaboration between human factors specialists, regulating authorities and industry.

REFERENCES

Bailey, R.W., (1982) Human Performance Engineering: A Guide for System Designers, Prentice-Hall Inc., New Jersey.

Bainbridge, L., (1983) Ironies of Automation. Automatica, Vol. 19, No. 6, pp 775-779.

Health and Safety Executive (1987) Programmable Electronic Systems in Safety Related Applications. Vol. 1: An Introductory Guide, Vol. 2: General Technical Guidelines, HMSO, London.

Marshall, C., Nelson, C., and Gardiner, M.M., (1987) Design Guidelines, pp 221-276 in Applying Cognitive Psychology to User-Interface Design. M.M. Gardiner and B. Christie (Eds) J. Wiley and Sons.

Meister, D., (1971) Human Factors: Theory and Practice, New York., Wiley.

Safety and Reliability Directorate (1985) Guide to Reducing Human Error in Process Operation. Short Version. U.K. Atomic Energy Authority, SRD R347, February 1985.

Wickens, C.D., (1984) Engineering Psychology and Human Performance. Columbus, Ohio, Charles Merrill.