Reducing the chance of information failures in the control room through better prevention management

by

Dr Linda J. Bellamy
White Queen BV, Postbus 712, 2130 AS Hoofddorp. The Netherlands,
Tel/fax +31 (0) 23 56 51353
e-mail: linda.bellamy@whitequeen.nl

Introduction

Some examples of chemical accidents from major hazard installations involving human failures in the control room have been examined. These failures are primarily recovery failures and can be attributed to poor information design. Since the same kinds of incidents appear to repeat how can solutions be found that can prevent the realisation of weaknesses in design?

Possible safety management solutions might include:

- Incorporation of a Human Factors philosophy or key Human Factors principles into policy documents in the design and operations phases, ensuring lessons learnt from previous accidents are considered in design and operations reviews

- Implementation of these HF principles and subsequent monitoring as an activity of the Safety Management System

Accidents

In 1988 a study was undertaken to address amongst other things the causes of accidents involving computer controlled processes. Operators concerns included:

- the proliferation of alarms
- fault diagnosis difficulties
- power failure response and switchover to manual control or ESD
- the role of the operator in the system
- system complexity and its comprehension by design operations and maintenance personnel

15 years on the same concerns exist and the same causes of problems seem to arise.

Human errors were associated with 59% of cases which were primarily caused by inadequacies in the information supplied to operators (Table 1)

	ACCIDENT NUMBER																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
CAUSE CONTRIBUTOR																	
Interface does not display actual status of plant or process	x				x		x									x	
Installation error leads to incorrect information		X					x										
Alarm set incorrectly			x														
No alarm (maintenance)			x	x													
No alarm (design)			x	x													
Operator misses information (overload)												x		x	x		x
No independent means of cross checking provided	x	X			x											x	
Operator fails to cross check							x										
Trip disabled/manual override	x						x			x							
Over-reliance on computer								x		x			x				
Inadequate knowledge										x							
Failure to update operators information											x						x
Incorrect control signal (maintenance)									x								
Design error: plant			x	x			x										x
Design error computer controlled system						x											
Software error						x		x									
Equipment hardware				x								x	x	x	x		
Computer hardware						x										x	
Connection hardware: electronic					x												

Table 1: Causes of 17 accident in computer controlled processes

Examples:

Accident 1:

Final error: Bottom discharge valve of reactor not closed when batch job started resulting in a release of a toxic gas.

Causes: The system was originally a software interlocked system. However the operator disabled the switch because it was oversensitive and presumably the system was always tripping. By disabling the switch the valve in question was taken out of the interlock. The result was that the interface did not display the actual valve status and no facilities for cross checking existed. At the moment that the batch job was started the wrong valve status was displayed. The operators forgot that a special case applied to this operation.

Accident 12

Due to a compressor failure a unit was shut down according to a standard procedure. However during the shutdown a compressor on another unit nearby tripped and, as with the first unit, a manual valve needed to be opened. This trip however was overlooked resulting in a release of a flammable chemical to the atmosphere. The operator received so much information at once from the process computer because of the shutdown operation that he missed the second compressor trip.

Accident 15

Damage occurred in a chemical plant due to exposure of equipment to extremely high temperatures. An operator failed to recognize a low level alarm in the cooling system because his attention was focused elsewhere. Only a restricted part of the process could be monitored on the screen and the operator was only watching what was happening in the furnace. Alarms were shown on another monitor. This was a scrolling display such that only the last 12 alarms were indicated. For a big event with lots of alarms being triggered this meant that the operator lost control of what went wrong and where.

A quick scan of short reports in the MARS data base of the EU's Major Accident Hazard Bureau using control room or human error as a search terms identified similar problems to those in Table 1 with operators' information following the occurrence of accident initiators. Significantly, it also revealed a surprising number of cases where the integrity of the control room had been impaired by the accident due to physical damage or entering of gases.

Recently I was given a description of a accident in which 3700 alarms went off in the control room without any prioritisation (the initiator occurred during start-up). A video link to the equipment which had failed was not looked at by operators for 20 minutes by which time a big cloud of flammable gas was floating over the site. In a case like this (during start-up) how can critical alarms be separated from non critical alarms? And even if that is possible, how to deal with that when 3700 alarms are going off?

When accidents have severe consequences and detailed investigation reports can be examined the human-computer interaction aspects as contributory failures can be much better regarded in the overall context of the design and management of the plant. It is not necessary to have yet more examples of accidents to see what is going wrong at the man-machine interface level. What is needed are approaches to deal with these problems at a deeper level. Amongst lessons learnt from an explosion and fires at a refinery in the UK were lessons that should have been already learnt:

- Display systems should provide an overview of the condition of the process
- Safety critical alarms should be distinguishable from other alarms, limited to the number an operator can monitor

Recommendation 1 of HSE's investigation was that

- Safety management systems should include means of storing, retrieving and reviewing incident information from the history of similar plants.

In addition it was found that instrument maintenance had been poor with the finding that instrument loops most closely related to the accident included calibration errors, incorrect information (inaccurate data sheets), and inoperability . Some of the faults were design related but others were known or could have been easily determined by inspection.

Recommendation 2 was that:

- Safety management systems should have a component that monitors its own effectiveness.

Neither of these are new concepts.

How can we, as human factors specialists, give good advice on how to avert these human recovery failures in operating plant? Are the companies stubborn or are we just not very good at solving this safety problem?

Philosophies and standards

A company needs basic philosophies and standards based on existing guidance and good practice. The basic ergonomics guidance has been around for a long time. More recently though there in abundance of information springing up. Is it being used?

Many companies find it very difficult to understand how to demonstrate the sufficiency of their provisions for human performance in the control room. Can they show, for example:

- What design standards and human factors assessments have been applied
- In-house ergonomics standards for displays and controls and for workplace design?
- What are the alarm handling design and procedures?
- How have monitoring and control functions been allocated been automation and operators?
- Have operators been involved in the design?

Having recently been asked to comment on a control room review I expressed my frustration that every time we undertook such a review the company failed to provide an indication of its own control room philosophy. Surely by now they could have developed one especially as they put such high store on human factors reviews early in the design process. One answer I was given was that establishing, maintaining, updating and distributing a centralized standard on human factors in control rooms design was an arduous task and it was considered preferable to "reinvent" this locally whenever there was a new design. Is that true?

To what extent can or should the Safety Management System inform on an appropriate philosophy of approach in the design and operating phases. Problems in the design phase arise for the human factors reviewer because, for example, decisions are made about control room design without recording why and the general approach to considering human factors in the control room as it relates to safety tends to be vague and does not seem to follow a consistent philosophy or standard of approach. There is no clear auditable trail.

When concentrating on assessments of safety critical issues, this is not well supported by systematic well tried assessment techniques when looking at control room issues, particularly display and control design. However, even a simple checklist review of a design or of operating plant, especially in considering responses to abnormal events from the lessons learnt perspective, would be a big step forward. This could involve all the people in the design process who impact ultimately on human performance, or operations and maintenance personnel associated with control room information. Can this not be part of the safety management philosophy, built into the company's review cycles?

Since most "control room" accidents seem to be related to recovery failures it seems logical that testing the provisions of the system should bear some relation to the sorts of foreseeable scenarios that could arise, including cases where information received may actually be incorrect. To what extent the testing of interface design in relation to possible scenarios is actually carried out is not clear, or even whether methods to do so exist in suitable form to be accepted and applied by companies.

Control room accidents are mainly pressure or temperature related as causes. The possible causes underlying the build up of an overpressure in a reactor vessel, for example, was described by one company as "countless" and in tracing back causes one can end up eventually in the feedstock tanks. Normally operators are expected to correct deviations before a plant goes beyond that into an area which is normally expected to be controlled principally by automated systems. This area of abnormal deviations has been described as a "no man's land". Does that mean that what happens out there is anyone's guess?

Taking the directly related components and process media for a reactor vessel for example, is it not possible to analyse, together with involvement of the workforce, what might be the deviations which could occur which lead to overpressures, and what would be available for and required of the operator for handling these deviations. Such an analysis could look at:

- Pressure
- Flow
- Temperature
- Percent measures such as level or valve position
- Position such as open-closed
- Analysers (eg. for concentration)
- Logic signals (on-off/yes-no signals)

where such instruments can be:
- an indicator
- a controller
- an alarm,
- a signal for an interlock system (mostly a shut down signal
- a combination of the above

How have the functions between operators and automatics been allocated? Is that as expected for the selected deviations? Is there sufficient information for diagnosis? How is it displayed? (etc.). Methods which get operators involved in looking at the systems they are familiar with in new ways always seem to provide benefits. So, how often are operators involved in some kind of assessment or review? Does the management philosophy encompass this?

Feedback

There are plenty of examples of information failures in the control room but why aren't the lessons learnt? Why is there such poor feedback of operational experience in new designs? In many cases the personnel who will be in charge of the control room operations are involved in the design process. But that all essential closing of the safety management loop for the design process – collecting and evaluating human factors experience from previous designs seems too often to be missing. In the operational phase, are operational reviews of the ability of operators to recover from initiators carried out in a systematic way? Or are they even carried out at all.

A safety engineer once said: "We don't know what our operators are thinking. If you can show us a way to get inside their skin that would be very helpful.

A psychologist once pointed out that:
"If you want to know what is wrong with the patient, just ask him".

References

Belke, James C. "Recurring Causes of Recent Chemical Accidents," proceedings of the International Conference and Workshop on Reliability and Risk Management, September 15-18, 1998

ISO 11064 Ergonomic design of control centres

Huppes, G. (1998) Werken in meld- en controlekamers. SDU Uitgevers, Den Haag [Working in control centres and control rooms – includes listing of norms]

Control room design – Technical measures document
www.hse.gov.uk/hid/land/comah/level3/5C991BC.HTM

Better Alarm Handling, Chemical Information Sheet 6 (2000), HSE Books (available free via HSE Books website www.hsebooks.co.uk)

EEMUA (1999) Alarm systems, a guide to design, management and procurement, Engineering Equipment & Materials Users Association publication No 191. ISBN 0 8593 1076 0.

Nicol, J. (2001) Have Australia's Major Hazard Facilities learnt from the Longford Disaster? An evaluation of the impact of the 1998 ESSO Longford explosion on the petrochemical industry in 2001, ISBN 085825 738 6, Institution of Engineers, Australia, 2001

Pitblado, R.M., Bellamy, L.J., Geyer, T (1989) Safety assessment of computer controlled process plants. Paper 46, 6th International Symposium Loss Prevention and Safety in the Process Industries, Oslo, June 1989.

HSE (1997) The explosion and fires at the Texaco Refinery, Milford Haven, 24 July 1994

European Process Safety Centre (2000) SHE Management systems for small to medium-sized enterprises. IChemE, Rugby, Warwickshire.

Bellamy, L.J. (2000) AVRIM2 Beoordelings en inspectiemethodiek versie 2000, Dec 2000. SAVE, Apeldoorn, The Netherlands, report 010432.G62 (see also www.savrim2000.com)

Abnormal Situation Management: A joint research and development consortium
http://www.asmconsortium.org/asm/dashboard.nsf?Open

Annex 1: Technical inspection points concerning control rooms from the Dutch AVRIM2 methodology

These points were generated by inspectors in the Netherlands who undertake inspection of Seveso II sites.

Control room

[ ][-][+] : Indications of operational problems? (such as controls switched to manual are possible indicators of operational problems)
[ ][-][+] : Controls for taking equipment in/out of service, automatic or manual
[ ][-][+] : Status of continuous alarms
[ ][-][+] : Settings
[ ][-][+] : Indications of procedural problems? (such as hand-written information, hand-written process schemas displayed on boards)
[ ][-][+] : Operational instructions for operators
[ ][-][+] : Operations manual
[ ][-][+] : Procedure for taking equipment in/out of service
[ ][-][+] : Instructions for rapidly taking equipment in/out of service
[ ][-][+] : Procedure for carrying out temporary tasks
[ ][-][+] : Procedure for deviating from process operations
[ ][-][+] : Procedure for dealing with an unknown situation/deviation
[ ][-][+] : Prevention of deviating from the correct order for adding substances
[ ][-][+] : Prevention of too high or too low temperature, pressure, agitator speed
[ ][-][+] : Prevention of entry of water, air, foreign substances
[ ][-][+] : Bypassing procedure
[ ][-][+] : Utility failure: (emergency)stop
[ ][-][+] : Present and up to date instrument and control diagrams and logic diagrams
[ ][-][+] : P&ID's: those which are used in the control room, up-to-date
[ ][-][+] : Clear overview of process and equipment descriptions
[ ][-][+] : Information of safe isolation of (in) active systems (list of blinds)
[ ][-][+] : Information/registration of safety bypasses
[ ][-][+] : Hazards are clear
[ ][-][+] : Safety measures are clear
[ ][-][+] : Information on temporary measures
[ ][-][+] : Double check on critical operational actions
[ ][-][+] : Spill measures provided
[ ][-][+] : Physical and chemical information necessary for the assessment of the dangers (flame point, boiling point, etc.)
[ ][-][+] : Procedure for shift handover
[ ][-][+] : Shift handovers
[ ][-][+] : Shift reports/shift log/communication at shift changeover
[ ][-][+] : Registration of safety information in the shift log
[ ][-][+] : Administration relating to safe work permits
[ ][-][+] : Check last 10 work permits
[ ][-][+] : Communication (resources) with the field
[ ][-][+] : Clear overview of safety bypasses
[ ][-][+] : Clear overview of protection bypasses
[ ][-][+] : Alarm signals (signal lamps on/off)
[ ][-][+] : Information on temporary measures
[ ][-][+] : Clear overview of emission points
[ ][-][+] : Accident overview
[ ][-][+] : Clear overview of interlock/trip/alarm equipment (position in the field, position on the graphics, settings)

[ ][-][+] : Clear overview of the consequences of loss of air, steam, electricity and cooling water
[ ][-][+] : Availability/use pf personal protective equipment
[ ][-][+] : Protection of buildings against the effects of explosion
[ ][-][+] : Ventilation
[ ][-][+] : Limited entry
[ ][-][+] : Minimum manning
[ ][-][+] : Supervision of operations

Annex 2: Human factors motherhood statements for the major hazard control room

Developed by Linda J. Bellamy and Tim A.W. Geyer based on human factors principles and lessons learnt from control room accidents

(A) Are operators provided only with information that they need and none they do not need?

(A1) Carry out task analysis to determine information and control needs.
(A1.1) Make sure these needs are met in the design.
(A1.2) Make sure these needs are met in training.
(A1.2.1) The operator should understand how the computer works for situation. where there could be a shared allocation of function.
(A1.2.2) Provide operators with training experience of controlling the plant with certain major control functions unavailable.
(A1.2.3) Provide operators with experience of having to complete tasks under conditions where a number of important tasks are competing for attention.
(A1.2.4) Provide the operator with hands-on experience in taking over from automatics. Use a simulator If necessary.
(A1.2.5) Provide training in generic problem solving strategies for fault diagnosis that can be used if an unusual unanticipated failure event occurs.

(A2) Avoid nuisance alarms. Alarms should be reserved for abnormal conditions.

(A3) Ensure as far as possible that information provided is accurate.
(A3.1) Measurement of equipment status e.g. valve open should, when possible, be taken directly from the equipment and not from the control action.

(A4) Criteria for action should be very clear for the following:
(A4.1) To take over from automatics.
(A4.2) To hand over control from the usual operator to the supervisor.
(A4.3) To shut down

(A5) Priorities should be clear
(A5.1) Prioritise alarms (use coding).

(A6) Alarms should be sequenced is a way which enables the development of an event to be better understood.

(A7) Procedures should Indicate appropriate operator actions in the event of loss of an important control function

(A8) Procedures should indicate appropriate operator actions in the even of Lose of an important control function.

(A9) Consider what information and control provision must be available in the event of a control room evacuation or total loss of all the operators computer display and control facilities.

(B) Is all the information relating to a particular task, as far as possible, 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 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 the 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
(B.3.1.1) Sufficient VDUs should be available for simultaneous display of the required information if it Is likely to appear on different display pages.
(B.3.1.2) 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 par 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 whore the relationship between 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.)
(B.4.1.1) 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 console.
(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.
(67.2) Group alarm summaries in a meaningful way (i.e. according to sequence, priority, function etc.)

(B7.3) Locate acknowledgement devices such that alarms cannot he 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).

(C) Operators' experience affects the way they read a display or operate a control. Have their expectations been violated as they move from one physical location (or VDU page) to another?

(C1) Be particularly careful if::
- A mix of vendors is used
- Different teams design different interfaces

(C2) Manual control actions carried out at one location should have the same effect as exactly the same actions carried out at a different location.
(C2.1) Keystroke actions to produce a particular effect should be the same at all work stations.

(C3) Display characteristics should be consistent between locations (or VDU pages)
(C3.1) Colour coding should have the same meaning across all displays.
(C3.2) Schematics should have similar formats (e.g. process flow is always from left to right). Thus maintain. as far as possible an exact spatial mapping of one display onto another.

(C4) VDU and panel display information layouts should be spatially compatible with one another. As far as possible, design the VDU displays first.
(C4.1) When changing over from a conventional to a computer controlled system design all the displays from first principles. Do not use old display formats as a basis for VDU or back-up hardwired displays; they may have been badly designed.

(D) Is the design of the interface compatible with the operator's limitations and capacities as an information processor?

(D1) The required skills of the operator should be known and then obtained, as far as possible, through selection, training and refresher training.

(D2) Try to avoid exceeding memory capacity.
(D2.1) Have fast methods of calling up a display.
(D2.2) Avoid operators having to page through several displays before they can get to the page with the information they want; it should be possible to call up any other page immediately, whatever the current page location.
(D2.3) Avoid the need to keep cross-referencing between different display pages.
(D2.4) All controls and displays should be clearly identified.
(D2.5) Use simple memorable codes that are easily distinguishable.
(D2.6) Include rapid information updating so that the operator does not have to wait.
(D2.7) It should not be possible to cancel or shelve alarm indications until the condition has been made safe.
[D2.6) There should be obvious reminders in displays when automatics have been manually overridden or disabled.
(02.9) Avoid scrolling alarm displays.

(D2.10) Ensure sufficient time for operators to update their working memory at the following times:
- At shift changeovers.
- When additional manning must be used (e.g. in emergencies).
- When following process changes. computer actions etc.

(D3) Try to avoid exceeding the operator's attention span as far as possible. Make the best use of his attentional capacities.
[D3.1) Avoid distractions
(D3.2) Frequently used and important displays should be placed in the operator's central viewing area.
(D3.3) Ensure alarms are not so frequent that they cease to have an attention getting effect.
(D3.3.1) Use meaningful alarm groupings so the operator will be able to deal with a large number of alarms, should they occur.
(D3.4) Avoid tasks competing for attention.
(D3.4.1) Have clear task priorities.
(D3.4.2) Use priority coding for alarms.
(D3.5) It should be possible for each alarm to gain the operators immediate attention (even it he Is not able to deal with it immediately).

(D4) Try to keep within the operators physical capacities.
(D4.11) Controls should be placed within easy reach.
(D4.2) Any displays (including VDUs) that must be viewed from the normal operator position should be easy to read.
(D4.2.1) Operators displays should. as far as possible, be within the operators visual field, not obscured by anything in the way and large enough to be seen from the required distance
(D4.3] Guard against inadvertent operation (especially single key actions which could have serious effects).
(D4.4) Avoid making Information difficult to read.
(D4.4.1) Avoid presenting information that is too small, low in colour or brightness contrast or confusable with neigbbouring information.

(D5) Analyses of the display provisions should be carried out with the involvement of the operators who are to use them.

(D6) Avoid ambiguity.
(D6.1) Take special care not to cross over pipe routings in schematics.
(D6.2) Take special care with coding. Each code must be unique.
(D6.2.1) Different alarms should have a unique code if a unique type of response is required. Colour should not be the only means of distinguishing between alarm and non-alarm conditions.
(D6.3) Labelling and other information should be obviously associated with the appropriate items.
(D6.3.1) On schematics. make use of space around display information. rather than drawing boxes, to distinguish between sets of data.

(E) Does manning meet resource requirements? Personnel should not be predominantly either overstressed or bored.

(E1) Examine the effects of an absent supervisor/operator etc. even if absent only for a short time

(E2) Consider whether manning levels, skill and experience will be sufficient for all known failure conditions.

[E2.1) Consider manning implications for worst case scenarios.
(E2.2) Consider manning for normal conditions.

(E3) Allocate tasks according to skills and experience.
(E3.1) Do not allow personnel with insufficient skills or capabilities to handle important tasks even temporarily.