Lessons learned from a disaster

Ian Nimmo & John Moscatelli, User Centered Design Services, LLC, USA, reflects on how learning from past experience has helped improve alarm management systems.

Over many years control systems and methods for implementing process control have been evolving. However, poor alarm management practices have been continuing for over 10 years, and it has not yet been possible to change the way people configure and use alarm systems.

The UK HSE and the USA OSHA regulators have both provided guidance and applied standards, yet this advice is often ignored. When alarm management is addressed in isolation a company will receive minor benefits, but most will never remove the latent errors inherent in the system. As can be seen from past incidents, it is not just the alarm system that fails in a disaster. Like most catastrophic incidents, it is just one of many management system failures.

Although there is a reluctance to solve this problem, it is not too difficult a task for most companies. However, when the facts behind the problem are examined, it soon becomes evident that it is not specifically the system at fault, but the way the system is used. For many years the tendency has been to put the system in automatic, wait for it to fail and then react to the problem. Just changing the alarm system will not change this behavior, which will crave more and more reactive tools, often entailing the addition of more alarms. During normal operations this may not be too problematical. However, alarm paralysis, where operators just accept or silence alarms out of habit, is frequently witnessed.

This becomes a real problem during a disturbance when all these alarms become active and the operator becomes too concerned with details to gain a view of the whole. As the incident worsens, the alarms become more frequent until an avalanche overtakes the operator, making the alarm system totally unusable. The tool now becomes part of the problem as it slows the communication between the operator and the controller, demanding time and resources while the continual audible alarm inflicts additional stress on the operator. When this occurs the chances of human error dramatically increase as operators miss important information. It can be seen from the following incident how the alarm system contributed to the problem. The incident also clearly demonstrates the impact of a badly designed user interface.

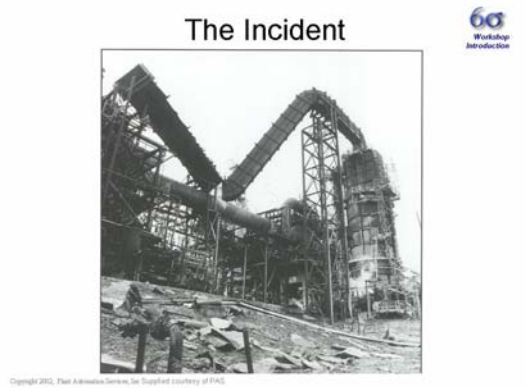
If this type of incident is going to be prevented, it will be necessary not only to resolve nuisance alarms, but also to change the operating culture and design a system for ‘situation awareness’. This is proactive, predictive and uses the alarm management system as an integrated tool that supports a good user interface or human computer interface (HCI). Before this article focuses on the new operating stance, the implications for the alarm system and the HCI, the incident will be reviewed.

The incident

An explosion, followed by a number of fires, occurred at 13:23 on Sunday 24th July 1994, on the Pembroke Cracking Company plant (PCC) at the Texaco refinery, Pembroke. The start of the events that led to the explosion can be traced to the period before 09.00 on that day, when a severe electrical storm caused plant disturbances that affected the vacuum distillation, alkylation, and butamer units as well as the fluidized catalytic cracking unit (FCCU). The crude distillation unit that provided feed to the PCC units was shut down as a result of the fire, which had been started by a lightning strike. During the course of the morning, all PCC units except the FCCU were shut down. However, the direct cause of the explosion that occurred approximately five hours later was a combination

of failures in management, equipment and control systems during the plant upset.
These led to the release of about 20 t of flammable hydrocarbons from the outlet pipe of the flare knock out drum of the FCCU.

The released hydrocarbons formed a drifting cloud of vapor and droplets that found a source of ignition approximately 125 yards from the flare drum. The force of the consequent explosion was calculated to be the equivalent of at least 4 t of high explosive.



This caused a major hydrocarbon fire at the flare drum outlet and a number of secondary fires. The site suffered severe damage to process plant, buildings and storage tanks. 26 people sustained injuries onsite, none serious. Rebuilding the damaged refinery cost an estimated US$ 75 million[1].

The cause

The incident was caused by flammable hydrocarbon liquid being continuously pumped into a process vessel that had its outlet closed. The only means of escape for this hydrocarbon once the vessel was full was through the pressure relief system and then to the flare line. The flare system was not designed to cope with this excursion from normal operation and failed at an outlet pipe. This released 20 t of a mixture of hydrocarbon liquid and vapor, which subsequently exploded.

The situation was caused by a combination of events, including:

- A control valve being shut when the control system indicated it was open.
- A modification which had been carried out without assessing the consequences.
- Control panel graphics that did not provide necessary process overviews.
- Attempts to keep the unit running when it should have been shutdown.

In their attempts to restore the plant to normal operation on the day, the company failed to take the necessary overall perspective, concentrating instead on the local, immediate symptoms rather than looking for the underlying causes. Furthermore, some arrangements for Management of health and safety were shown to be inadequate, illustrated by failures in company systems for: assessing the risks from plant and procedural modifications; the use of programmable electronic systems (PES); and management of inspection and maintenance.

Issues with human factors

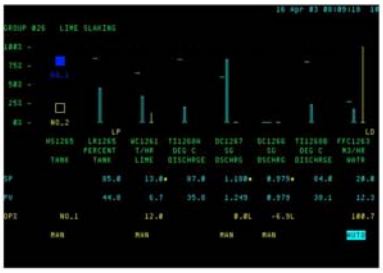
The incident developed from its initial causative problems due to the combined effects of two factors. Firstly, operators were not provided with information systems configured to help them Identify the root cause of such problems. Secondly, the preparation of shift operators and supervisors for dealing with the stressful situation of a sustained upset was inadequate. The interface between the operators and the control system should have been designed to give the operators and managers overview facilities through the display.
This was not the case, and the discrepancies in mass and volumetric balance in the process that would have provided a powerful indication of how the problems should have been dealt with were not noticed. Some managers and supervisors were involved in ‘hands on’ operational matters instead of performing a strategic and diagnostic role. This resulted in action being concentrated on the symptoms of the problem, and not the causes.

Issues with operating displays

Under the FCCU control system that existed on the day of the incident any imbalance in liquid flow through the FCCU could lead to liquid accumulation. It was therefore important that any imbalance in liquid flow be detected so that the mass flow of the unit could be returned to a balanced position. The plant was well equipped with alarms, which showed where liquid was accumulating, but it was more difficult to assess the relative flows through the vessels and the overall mass balance of the unit. The process of fractional distillation requires that one raw material is divided into many fractions. While it

was easy to assess the unit feed rate, the various outputs of the process were spread over five product streams. This generated a practical problem, in that the accumulated outputs of the system may be spread across several different control display units, and the overall output of the unit would not be readily apparent unless the control system were configured to meet this need.

Typical Group Display



Unfortunately, this need was not met. There were no displays providing an overview with an appropriate time scale on the FCCU. Therefore, it was difficult to obtain a complete picture of the whole or large sections of the process.
In a primarily display screen based operating system, the provision of good overview displays is of particular importance, as the operator does not have a continuously available set of panel indicators. During the incident no one from the operations department had a complete picture of the FCCU. The actual FCCU graphics on the operating displays were not best designed or configured to help operators control the process:

- The operating graphics on the FCCU contained limited amounts of process data per graphic, and did not make use of color and intensity to highlight process data.
- Some graphics contained details of the internal structure of plant items. However, displaying the structure of plant items is only useful if measurements or derived information (e.g. pressure, flow, temperature) are also displayed to give the operator information relevant to the plant status.
- At times the text was unnecessary in the FCCU graphics. Text takes up large amounts of space on a graphic and there were instances where the same information could have been better indicated by color change.

Recommendations by the HSE

The Health and Safety Executive made 22 recommendations dealing with safety management systems, human factors, plant design, plant modifications, inspection systems, and emergency planning. The three Recommendations on human factors are of immediate interest in the design of the control room working environment.

Recommendation three

Display systems should be configured to provide an overview of the condition of the process including, where appropriate, mass and volumetric balance summaries.

Recommendation four

Operators should know how to carry out simple volumetric and mass balance checks whenever level or flow problems are experienced within a unit.

Recommendation five

The training of staff should include:

- Assessment of their knowledge and competence for their actual operational roles under high stress conditions.
- Guidance on when to initiate controlled or emergency shutdowns and how to manage unplanned events, including working effectively under the stress of an incident.

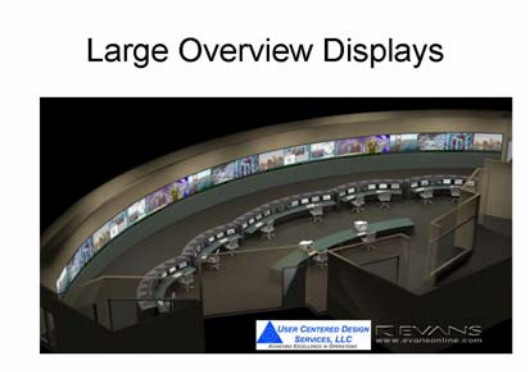
The solution

To eliminate this type of incident, rationalizing and suppressing a few alarms is not sufficient. Firstly, the operating stance and the way operators behave over a 12 hour shift must be changed. To change a culture is difficult, requiring substantial management effort, resetting values and beliefs, enforcing new policies and management systems and not accepting poor performance.

The HSE document recommendation number five focuses on training and stress management and it is important that each job should have a job performance profile. Many companies have focused their process control or console operator training to a few good, competent, management selected employees who volunteer for this dedicated role.
When the role is not dedicated, the position is often filled by someone who does not have enough outside knowledge or experience, and is not always competent or suitable for the type of work. A few companies are investing an extra nine hours in testing for this position which includes psychometric evaluations together with important skill tests that address core competencies for this critical position.

In the past, control rooms or user interfaces have not been designed to ensure good situation awareness and to meet today's best practices. In fact, the biggest draw back to meeting these new

goals is people's reluctance to change.

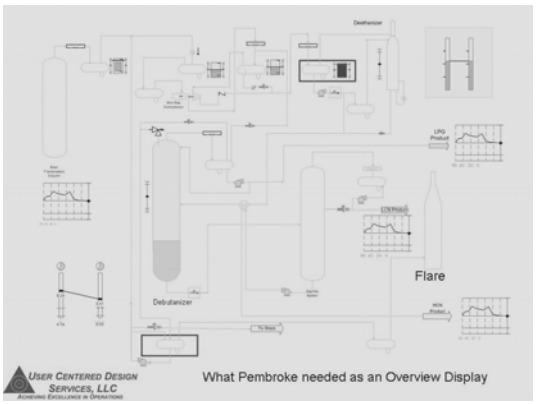


The operators usually want to stay with what they have, even though it has major problems and limitations that cause them to err. Control engineers, who often believe that operators need an exact copy of what they have, can be a barrier to progress. Even though a change in DCS technology demands a rewrite of the user interface they try to imitate what they already have to avoid new training and design work. Many control engineers see system changes as an admission that the old systems they designed were poor, rather than evolutionary application of new technology to improve the control system.

The high error rate and the reactive stance are contributing factors to disasters, like the one described in the case study. To be successful in this area operators must first be informed of the need to change. Incidents like those in the case study can be eliminated, and there are major benefits from operating differently.

A recent case study comparing traditional user interface to the new HCI techniques described in the EEMUA 201 document demonstrated a 35 - 48% improvement in what was identified as good console operators. They recognized problems faster and more consistently. This impacts the bottom line and reduces the number of abnormal situations an operator has to deal with.

To address HSE recommendation number three, concerning the lack of overview displays and the mass and volumetric balance summaries, it must first be understood what an overview display should contain and who it is intended for. The display should contain a view of the operator's whole scope of control (all process units being monitored and controlled by a single operator) with the most critical equipment and process KPI's, including calculated process conditions that need frequent monitoring. It should also include all critical, emergency and high priority alarms.



The designer needs to understand what process values and trends are relevant at this level of detail.

The current trend is to add mass energy balance information to this display, together with important production rather than process information. The display provides a good use of trend information, especially hourly averages which allow operators to track shift performance. The overview display is often placed on a large off workstation or video wall, depending on the display's audience. In a refinery, units are closely coupled through feed and product streams, heat integration and dependant utilities, so the overview of any given unit may be useful to multiple other units. The overviews are ideal for supervisors, engineers and managers. Refining has benefited from a new optimization or abnormal situation disturbance supervisor whose goal is to optimize the whole refinery and make dynamic decisions based on performance or disturbance management, managing steam, electrical power and other common utilities. However, in chemical plants those are more independent and do not have the interactions with other units, smaller local overview displays that are directed to one or two operators only are used.

This new HCI paradigm demands that the control system displays are designed to support the tasks required of the primary users, the operators, not the managers or the engineers. To support this, a graphic hierarchy is needed where the operator can drill down to get additional levels of information, as they are required for the task at hand. The overview, or level one display, provides the big picture overview, whilst the unit view or level two display, provides access to a process flow diagram level of information, including access to the key controllers. The operator will make most of the control moves from this display level. The detailed view, or level three display, are the traditional P&ID level displays most systems rely on today, which contain all the I/O available. These displays are used for detailed troubleshooting, as they provide

a level of detail not often needed in day to day operation.

As the designer creates level two and level three displays, it is important, to have the correct levels of detail. The tendency in the past has been to create graphics that are life like, with 3D vessel and lots of detail around static data. This brings unnecessary fixed data to the foreground and forces important variable data to be crammed in and hidden in the background of the graphic.

Likewise, the use of multiple bright colors to indicate product flows is unnecessary. If an operator does not know or understand what is flowing in and out of the unit they should not be controlling it. Most operators can draw all their inputs and outputs from memory. They know normal flows, temperatures, pressures and comprehend what the process is doing. They do not need their displays over populated with details which are of interest to the managers and engineers. They do however need better awareness of the dynamic variables in the plant. It has also been discovered that displays need to be void of color. When a disturbance or process upset occurs color is added, using hue and intensity to prioritize information to the operator. Displays are now designed with hidden levels of detail so that the operator can drill into the information as required, rather than trying to cram all the information onto one screen.

The other final difference is the navigation techniques to move between displays. In the past, operators used to demand more and more screens, even though it was proved that they could not effectively use more than six screens during normal operation and three screens during a disturbance. They argue that the extra screens are useful to other operators or supervisors who help out during a disturbance, though this is not useful when that person is not available.

This new strategy tries to make operators proactive. With good HCI, dependence on alarms is dramatically reduced, allowing them to be rationalised and then physically cut, hence reducing the potential for alarm flood.

Each of these initiatives is dependant on management providing good direction through an EEMUA compliant alarm philosophy, an EMMUA compliant HCI style guide and designing the control room to reduce distractions and support good situation awareness. The design of all these systems should support operator vigilance and reduce stress.

References

1. A report of the investigation by the Health and Safety Executive into the Explosion and Fires on the Pembroke Cracking Company Plant at the Texaco Refinery, Milford Haven on 24th July 1994, HSE Books (1997), ISBN 0 7176 1413 1.

Contact information:-

Ian Nimmo
User Centered Design Services LLC
Tel. (623) 764 0486
Email inimmo@MyControlRoom.com
Web http://www.MyControlRoom.com