

Situation critical

Ian Nimmo, User Centered Design Services Inc., USA, discusses organisational accidents and abnormal situation management.

When there are problems in the processing industry, the industry responds to them with engineering solutions. This has been done by different disciplines for decades and has helped maintain a good safety record. However, in recent years accidents have been experienced that have some very common threads, that engineers are having difficulty designing out of systems.

The industry has tried to learn from major catastrophes such as Bhopal, Piper Alpha, Three Mile Island and Chernobyl, but it has been introduced to a new type of failure, which was categorised by Professor James Reason in his book *Managing the Risks of Organizational Accidents*. He stated in the first chapter that 'organisational accidents are rare, but often catastrophic, events that occur within complex modern technologies', and that 'organisational accidents are a product of recent times or, more specifically altered the relationship between systems and their human elements. Organisational accidents may be truly accidental in the way in which the various contributing factors combine to cause the bad outcome, but there is nothing accidental about the existence of these precursors, nor in the conditions that created them.'

The most important question to ask after the events that led to the large loss of life on the Piper Alpha Platform must be: how can this be prevented from ever happening again? One of the investigators clearly answered that question. He said the requirements for safe operation are:

- Hazards must be recognised and understood.
- Equipment must be 'fit for purpose'.
- Systems and procedures must be in place to maintain plant integrity.
- Competent staff must be employed.
- There must be emergency preparedness.
- Performance must be monitored.

As many of the more recent major accidents are reviewed it is clear these lessons have not been applied and the lessons learned in other industries such as the aircraft industry, which has many parallels to the process industry, have been ignored. If the industry would only apply the lessons learned about situation awareness it



Figure 1. The BP Texas City incident.

would have a different perspective on the alarm problem. It would better understand that alarms are just one of the tools that can be used for situation awareness.

Texaco Pembroke

Texaco Pembroke started as a simple instrument failure caused by an electrical storm. This was not the root cause of the accident that came later, as the operators attempted to restart the refinery. During this period one of the console operators on the cat cracker experienced a series of problems that gets rolled into a term called human error. This is partly to blame for the inability to fix the problem, a better term would be design induced errors. The simplest instrumentation system design failed at Pembroke, as a level in a knock-out drum initiated an alarm that was not responded to by the operator. This is pretty basic. However, the designers did not consider the reliability of the operator and the consequences of no response by the operator.

The UK HSE analysis of the incident determined that the DCS displays conveyed limited information and the operator became overwhelmed with alarm data as raw alarms were being presented at a rate of 20 - 30 per minute. The HSE determined that 'the flood of alarms greatly decreased the chances of the operators restoring control in the plant.' In the final 11 minutes, the operator received 275 alarms, of which 87% were categorised



Figure 2. Esso Longford fire.

as high priority requiring an operator response within 3 minutes for each alarm! Critical alarms were overlooked in the midst of other alarms.

So here the DCS Human Machine Interface (HMI) and the alarm system can be clearly identified as major casual factors behind this incident. To walk away from this incident and have a focus purely on the alarm system would be a grave mistake that many other plants would make.

Even the HSE's actions after the incident in some ways directed the industry to this conclusion as the HSE focused attention on an alarm management as they introduced their Research Report 166/1998 'The management of alarm systems.' The industry responded and brought out a new guideline on Alarm Management through the work of the Abnormal Situation Management Consortium and EEMUA with the EMMUA 191 document. Both documents were very effective and were really needed by the industry worldwide. However, nothing was done to raise the standards of the HMI (EMMUA 201 was not considered helpful) and this made it difficult to fully resolve the alarm issues, leaving the industry wide open to repeated incidents.

Engineers around the world responded by trying to fix the alarm management problems and are doing so at many plants. New standards and guidelines are now in place that define what 'good' looks like for alarm management. Yet, many still have not complied, and struggle to reduce and fix alarm management issues. Perhaps engineers are trying to solve the wrong problem or just the most obvious symptoms of a bigger problem.

Esso Longford

In Australia, Esso has a gas plant that, several years after the Pembroke incident, experienced a catastrophic failure in Longford. At the heart of this incident is a simple instrumentation failure that involved a level, an alarm and an expected operator action. The system failed and condensate overflowed the column and froze a heat exchanger. The incident may have been recoverable had the operations and maintenance team had basic training and been able to understand the dangers of adding heat and how brittle fractures are caused. The designers failed to consider the reliability of the operator and the consequences of 'no response' by the operator.

The Australian Royal Commission that investigated the

accident again made some important discoveries. They stated that the failure to undertake ongoing analysis and evaluate process trends within the gas plant diminished the likelihood that such upsets as those which contributed to the accident on the 25th September 1998 (operating conditions in the absorbers or condensate carryover) would be detected and avoided by appropriate responsive action. They also stated that it is evident that well before the accident, panel operators had become accustomed to the frequent occurrence of alarm conditions at the base of the absorbers. High level alarms had become frequent enough for such alarms to be regarded as a nuisance rather than a warning of process upsets requiring action. This goes some way in explaining the insensitivity of operators to such alarms in the lead up to the accident.

The practice of operating the absorbers in alarm had a bearing upon the loss of lean oil circulation. Excessive condensate carryover could not have occurred if operators had responded to the alarm warnings in the control room in the period leading up to the accident.

Operators would, no doubt, have reacted more appropriately to high levels in the absorbers had they appreciated the potential for condensate carryover and the dangers associated with cold temperatures, but even without this, the operators did know that operation of the plant for any length of time in alarm generally carried risks with it.

There was no evidence of any system to give priority to important alarms (even after the lessons of Pembroke). Good operating practice would have dictated that critical alarms be identified and given priority over other alarms. It would also have dictated that operators be informed of the correct way to respond to process upsets identified by the occurrence of critical alarms.

The lack of a system of priority for critical alarms explains why the operator failed to respond promptly or adequately to the activation of the alarm on the morning of the accident. Many lessons were learned at Longford and again poor situation awareness can be seen as a major contributing casual factor in the accident. It is fair to state that the control room had poor ergonomics, a very poor HMI. Operators did not use trends to predict process upsets or evaluate long term process trends or plant performance.

The lessons from Piper Alpha and Pembroke were ignored by Esso Longford, a mistake which surely the industry would not repeat?

BP Texas City

Unfortunately, in the next few years the BP Texas City disaster occurred with very similar circumstances. This time it was not an electrical storm but a plant startup after a turnaround. In conclusion, it can be determined that a simple instrumentation system that consisted of a level transmitter, an alarm and an expected operator response failed. The system failed and hydrocarbons overflowed and a catastrophic explosion was the result. The lessons from Piper, Pembroke and Longford were not learned. Without oversimplifying this accident, like many other organisational accidents many contributing factors can be found. However if the Piper Alpha's lessons for safe operation were applied they could have avoided this accident. It is apparent that the plant had poor alarm management practices, that the HMIs did not provide adequate situation

awareness. Again, a breakdown of the technological system and its human elements can be seen.

If several recent major accidents that have happened over the last 20 years are examined, it can be concluded that these incidents have multiple causal factors, but at the centre of these incidents there are reports of console operators missing important information. In recent analyses it has been identified that basic skills for monitoring the DCS have been compromised by data overload, misplaced salience, workload and other stress factors, such as fatigue.

Situation awareness

If the subject of 'situation awareness' is to be understood years could be spent doing research to come to the conclusion that it needs to be treated as a system and that the system has elements such as alarms, HMI, trends and ergonomically designed control rooms to reduce distractions, fatigue and allow operators to perform to their best performance.

With regards to the aircraft industry, as stated earlier, there are some sound definitions of 'situation awareness' and some sound engineering principals that have resolved many human error issues experienced by the aircraft industry. It can also be seen from that industry that trying to automate a way out of this problem is fraught with new problems such as increased system complexity, loss of situation awareness, system brittleness, and workload increases at inopportune times. The attempt to automate a way out of so-called human error has only led to more complexity, more cognitive load and catastrophic errors associated with losses of situation awareness (Endsley & Kiris, 1995).

So, to address this issue it is critical first to understand the full problem. The industry must examine why operators have failed in the past and be critical of the systems given to them and try to understand why these systems are not successful. This is extremely difficult as it clashes with many cultural issues and attacks many of the working practices that have evolved with the industry. What many engineers today hold onto as a good practice may be revealed as poor or bad practice.

It was a revelation to the author, as a traditional engineer who came up through the electrical engineering background, learned instrumentation and evolved into a control engineer after first working with early computers that evolved into what we know as DCS systems today, that the fundamental system design and growth through evolution was flawed.

In Mica R. Endsley's book *Designing for Situation Awareness: An Approach to User-Centered Design* she defines a technology-centered design that takes traditional sensors and systems that are needed to perform functions, then added a display for each system that informed the operator of how well that particular system was operating or its present status. As the design evolved systems kept on being added until the operator displays grew exponentially. The operator was expected to be able to find, sort, integrate, and process through the vast array of information that is available, leading inevitably to an information gap. It was never even considered that the human has limitations and that the human could become the bottleneck. As the display of data in these systems is centered on technologies producing them, it is often



Figure 3. Modern control room with ergonomic desktop and overview displays.

scattered and not ideally suited to support human tasks.

An alternative was never considered. Engineers were aware that in the old days when they first started instrumentation, they had panels with instruments mounted on them. The instruments were arranged around the operator's tasks so that the operator would not have to run up and down the panel every time they had to do a task. This was a better solution, though it had limitations in that the panel only had a certain amount of room for equipment and change was a difficult task, so was adding new equipment once the design was complete (built in MOC).

However, user-centered design goes much further than this basic concept of task grouping. It considers displaying information in ways that fits the goals, tasks and needs of the user, it strives to achieve optimal functioning of the overall human-machine system rather than information centered on sensors and technologies that produce it.

One of the first barriers that Endsley defines is understanding what user-centered design is not. This is going to be hard for many engineers, because over the years of developing HMIs and graphics, the engineer learned that the operator often had more insight into what was a good graphic than what they were producing therefore they either left the design entirely to the operator user or sought operator input into what the graphic should look like. This sounds very reasonable but has been found to be fraught with pitfalls and could be considered a poor practice.

Endsley brings out some important points that should be considered. The first is that operators often have only partial ideas about what might be better than what they are used to. They generally have very limited knowledge of how to effectively present information and design human interactions with complex systems.

The next is that these issues are compounded by the fact that most systems must be used by many different individuals, each of whom may have significantly different ideas on what they would like to see implemented in a new design. The result of this approach is an endless and costly cycle of implementing new ideas, only to have the next team of operators decide they want something different. Design solutions tend to be sporadic and inconsistent across features of the interface and many design problems are not recognised.

The best operator on the unit is often seen designing graphics and although much good thought has gone into

the design, inconsistencies can be seen such as poor use of colours, not reserving colours for coding or using colours for multiple codes, many more than most operators can memorise. Also poor layouts and cramped information are an attempt to get everything that could be possibly be of value on the display.

Endsley is not saying that the operators do not have valuable input, in fact she states that operators are a valuable source of input providing information regarding problems experienced, information and decision needs, working conditions and functions needed. The unfiltered implementation of whatever they want completely neglects the large base of scientific literature regarding the types of interfaces that work and those that do not.

That is the big one out of the way. The next idea she discusses is the well-meaning attempt to help manage the information overload problem is the idea of information filtering or trying to anticipate the information needed by the operator. The bottom line of this approach is that it puts the operator back in a reactive, rather than proactive operating stance, and influences the performance of both the operator and the system. Finally, her comment is that user-centered design is not making decisions for the operator or doing things for the operator. So what is it? The answer to that question can be found in the book itself.

Conclusion

With all this new insight, what is the bottom line here?

Today there are failures associated with breakdowns between technological systems and human partners. To fix this issue, the limitations, strengths and weaknesses of both partners must be understood. The strengths of both must be exploited. Having an operator waiting for an alarm before engaging in the system is a poor use of a human.

The human must work through a three stage approach which includes awareness, perception of the elements in the environment, comprehension of the current situation and finally the ability to predict what will happen next, projection of future status. To achieve this operators are needed that are tracking trends, responding to alarms when the trend or graphic has failed to make the operator aware of the situation and correct it before the alarm state. The human needs to comprehend by having displays that turn data into information.

For the operator to be performing to the new levels a control room environment is needed that is proactively supporting operator alertness, does not contribute to fatigue or distractions and supports the operator in all the tasks they have to perform. This includes non-DCS tasks such as report writing, MOC, performance improvement, training, etc.

With today's technologies, the operator no longer has to look through a keyhole at infinite data. They can provide goal/task based hierarchical information across large screen displays and an ergonomic desktop. This desktop will recognise the limitation of the human and will have no more than four working displays together with a permanent overview display. This means that the operator desk will also need to be ergonomic and the DCS vendor's traditional console will be a thing of the past.

Never again should an incident occur that has a major failure of the human due to overwhelmed operators that cannot respond to a simple level control alarm.

References

1. REASON, James, *Managing the Risks of Organizational Accidents*, Ashgate, ISBN 1-84014-105-0.
2. ENDSLEY, Mica R., BOLTE, Betty, and JONES, Debra G., *Designing for Situation awareness An Approach to User-Centered Design*, Taylor & Francis, ISBN 0-748-40967-X.
3. *The explosion and fires at the Texaco Refinery*, Milford Haven, 24 July 1994, HSE Books, ISBN 0 7176 1413 1.
4. *The Esso Longford Gas Plant Accident report of the Longford Royal Commission*, Government Printer for the State of Victoria, No 61-Session 1998 - 99.

DRAFT