THE MAGAZINE OF THE INSTITUTE OF MEASUREMENT AND CONTROL

INSTMC.ORG

TOO MUCH INFORMATION

FEATURES//

SIG SET TO DRIVE INNOVATION AND COLLABORATION

FUNCTIONAL SAFETY FOR MANAGERS

VALIDATING GAS MONITORING EQUIPMENT

SPECIAL INTERVIEW//

DR CLAIRE ELLIOTT MINSTMC

APRIL_2018_ISSUE SIX

PRECISION MAGAZINE

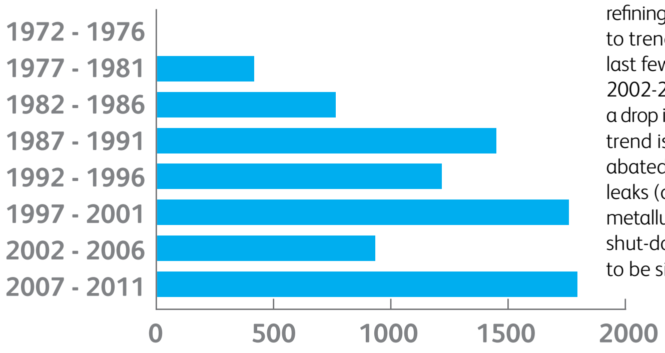
TOO MUCH INFORMATION

Dr Maurice Wilkins, Engineering Director of the InstMC, considers how Standards Based Decision Support can help operators with abnormal incidents.

Challenges Facing Process Operators

According to a 2012 report by the Energy Practice of Marsh Ltd, a division of Marsh McLennan, the 5 year loss rate (adjusted for inflation) in the refinery industry over the period 1972-2011 continued to rise, with incidents occurring during start-ups and shutdowns continuing to be a significant factor as shown in figure 1 below.

Fig 1: Refinery Losses 1972-2011



Five year loss total in the refining sector have continued to trend upwards over the last few years. While the 2002-2006 period presented a drop in losses, the increasing trend is unlikely to have abated. Piping failures or leaks (corrosion or incorrect metallurgy) and start-up and shut-down events continue to be significant causes.

These losses are occurring at a time when control systems and instrumentation on process plants have improved substantially. So why are they happening?

During normal operation, processes run mostly untouched by operators, especially in continuous plants. But if an incident occurs, there is often too much information, which increases operator mental workload and so they can become confused and make mistakes. Humans are not designed to cope with masses of information, especially when they are under stress. Start-ups and shutdowns of process units are considered to be 'normal' operations, along with grade changes and other transitions, however these are amongst the more error prone operations that again increase the mental workload of operators.

Texaco Refinery, Milford Haven

A clear example of extreme operator mental overload happened on Sunday 24 July 1994, when a lightning strike started a fire on the crude distillation unit (CDU), which eventually led to an explosion on the fluid catalytic cracking unit (FCCU). Although the media put the blame on the lightning strike, the incident report stated that "these events, though significant in initiating a plant upset, were not the cause of the release and explosion that occurred five hours later. These consequences resulted from subsequent failures to manage the plant upset safely". Luckily, although there were some serious injuries, no one was killed.

Amongst many other things, the report cited bad alarm management, bad display design and a failure to follow procedures. For example, it stated "From the limited amount of alarm information relevant to the event which was preserved from just one of the journals, it was seen that in the last 10.7 minutes before the explosion the two operators had to recognise, acknowledge and take appropriate action on 275 alarms. At times during the morning operators were doing nothing but acknowledging alarms". It went on to say that the chances of operators restoring control manually were reduced as the incident progressed due to them being overloaded by a "barrage of alarms". There were 2040 alarms configured and of those in the DCS 87 % were high priority. During the incident, the operators had to cope with alarms coming in a had to cope with alarms coming in a rate of one every 2-3 seconds, which resulted in many being cancelled due to their nuisance. There was no evidence that a vital high level alarm on the flare drum which went off 25 minutes before the explosion was ever seen.

In addition the report indicated that the FCCU graphics were not designed in a way that helped the operators to control the process. There were limited amounts of process data and colour was not used in a way to highlight important data. It also said that there was information on the graphics, such as the structure of plant items, which had no relevance to plant operation and shouldn't have been there. Finally, several procedures had fallen into disuse from lack of practice and documenting them. I will discuss later how standards and better design could maybe have helped in this incident.

Managing Mental Workload in a 'Life or Death' Incident

Many airline pilots are chosen due to their ability to handle stressful situations calmly and they go through extensive mental workload training on simulators, covering every kind of incident that could happen. In fact on the 'Miracle on the Hudson' US Airways flight 1549, which landed safely on the Hudson after a bird strike on January 15th, 2009, none of the crew had ever met each other, but their calmness and following procedures to the letter, saved the plane and many lives.

Can we use machines to guide humans and the deductive power of humans (given a logical number of options) to make the correct decision? Mary L. Cummings, Director of the Humans and Automation Laboratory (HAL), at MIT and a former Navy F-18 pilot, who is doing research into human-automated path planning optimization and decision support has said "Humans are doing a pretty good job, but they do it even better with the assistance of algorithms" and "This research is really showing the power of how, when algorithms work with humans, the whole system performs better." She maintains, letting computers analyse masses of information generated during an incident and giving the operator options as to how to alleviate the incident, may help to manage the mental workload.

Humans have emotions and get stressed. There is no better example of this happening than in a crisis, as illustrated by the Texaco case. Some humans are able to handle crises in a very calm way, as shown by historical heroic efforts in war and peace, but the majority tends either to try to do everything, panic or just switch off. So when even the best operator is faced with many alarms coming in at the same time and other things happening around him, he will likely try to look at as many as he can and work out a scenario and possible solution, but that may be too late. It would be much better if the system provided him with options and guidance – or decision support.

Standards Based Decision Support

Decisions are made by assessing the problem, collecting and verifying information, identify alternatives, anticipating consequences of possible decisions and then making a choice using sound and logical judgment based on available information.

Few humans in a crisis are able to do this without help. Either they find it difficult to manage the situation to give them time to gather enough information to make a sound decision or they just run out of time trying to make the decision. With decision support and guidance this task becomes more manageable.

In key areas such as human machine interface design, alarm management and procedure management basic decision support may be developed. In support of this, industry standards are either available or being developed. For now, I am going to concentrate on The International Society for Automation (ISA), a globally recognised standards development organisation, which is developing standards based on the three areas mentioned above. They are providing or will provide a good basis for decision support:

- ANSI/ISA-18.2-2009 – Management of Alarm Systems for the Process Industries
- ANSI/ISA-101.01-2015 – Human Machine Interfaces for Process Automation Systems
- ISA–TR106.01 – Technical Report: Procedure Automation for Continuous Process Operations – Models and Terminology
- ISA–dTR106.02 Working Draft 16 – Technical Report: Procedure Automation for Continuous Process Operations – Work Processes

ANSI/ISA-18.2, which has been a standard since 2009, provides requirements and recommendations for the activities of the alarm management lifecycle. The lifecycle stages include philosophy, identification, rationalization, detail design, implementation, operation, maintenance, monitoring & assessment, management of change, and audit. ISA18.2 has also been adopted by IEC and so is a recognised international standard.

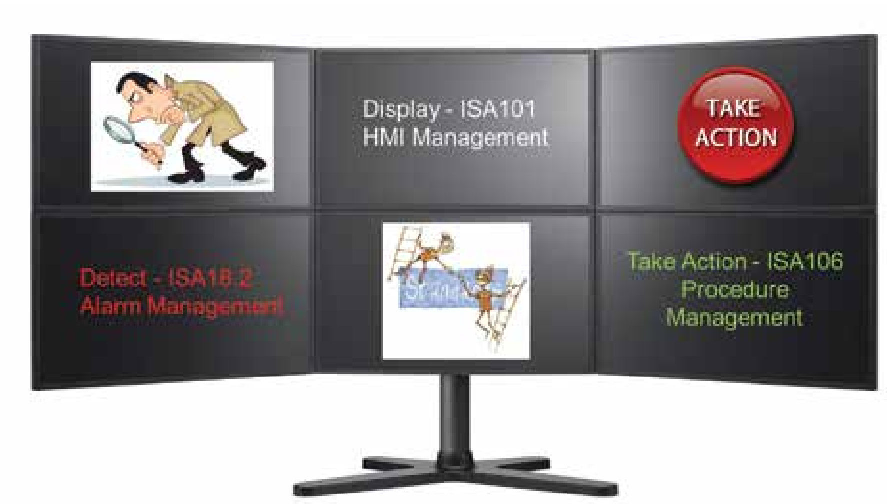
ANSI/ISA-101.01 has been a standard since 2015. It is directed at those responsible for designing, implementing, using, and/or managing human-machine interfaces in manufacturing applications. The committee is now developing technical reports showing how the standard can be applied.

The ISA106 committee has produced two technical reports, one addressing models and terminology and the other work processes. The committee will then develop a standard to provide good practices to address many of the human performance limitations that can occur during procedural operations. The technical reports as they stand give a good basis for us to start developing decision support systems.

Standards Working in Harmony for Decision Support

If configured correctly, well planned alarms could trigger procedures in many abnormal situations and a well-designed human machine interface could bring a developing incident to the attention of the operator in a timely manner. We call this Advanced Decision Support

Fig 2: Standards Based Decision Support



Alarm management should limit alarms to what the operator has time and ability to handle by developing an alarm philosophy and rationalisation program. The alarms should then be continuously monitored and optimised. In that way we can ensure the right alarms are detected and then either the operator or the system can take action.

With good HMI management, the operator displays are designed based on operator tasks and incorporate human factors such as colour, layout and navigation. They should provide situation awareness through trends and profiles and provide clear indications of items that need attention.

Finally, procedure management can help the operator to put corrective actions in place or actually take corrective actions automatically. It can also prevent actions from taking place if the initial set up is not correct for a start-up or transfer and so on.

The airline industry is amongst the safest and most automated in the world – in fact most modern aircraft would not be able to fly without the use of computer guidance, yet procedures play a big part in the way aircraft are operated. Pilots need to go through many procedures before, during and after a flight.

The first recorded procedures were introduced by test pilots in 1935 after a crash of the B-17 Flying Fortress almost caused the programme to be abandoned due to a gust lock still being engaged at take-off. It was said that the plane was too complicated to fly. The test pilots developed procedures for take-off, flight, before landing and after landing. Boeing delivered 12 of the aircraft to the Air Corps and they flew 1.8 million miles without a serious mishap. Every type of plane from small private planes to the largest jumbo jet now uses procedures for all aspects of the journey and not following them could lead to a pilot losing his licence to fly (or worse).

In the same way the start-up and shutdown of a process requires standard operating procedures (SOPs) which are designed to ensure the process is started up or shut down the same way each time. However, these are sometimes 'modified' by experienced operators who may see a better way of doing things. In the case of both the pilot and the process operator, there are ways that these improved procedures should be evaluated and turned into current practices. In the case of an aircraft, the consequences of not doing this are obvious, but in a process plant, a tweak here and a tweak there may go unnoticed until things go wrong. As with the operation and maintenance of aircraft, the goal of operations and decision support is to capture the knowledge of the best and hopefully calmest operator on his/her best day under all conditions.

Figure 3, below, depicts the methodology for capturing best practices procedures. The goal of this approach is to "distil" best operating practices and find the right balance between manual, prompted and automated procedures, documenting and implementing the procedures and then executing continuous improvement cycles on them. Automating every procedure does not always provide the best solution; neither does manually executing every procedure. What does provide the best solution is to consciously examine events that caused production interruptions, then examine the

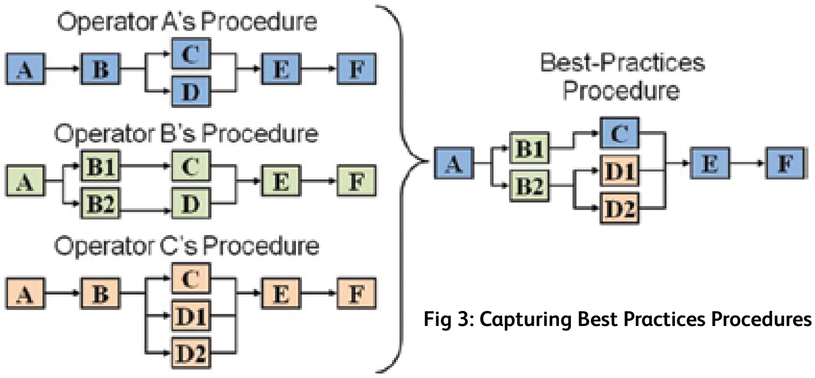


Fig 3: Capturing Best Practices Procedures

procedure operations associated with those events, document them and determine what type of implementation will provide the best economic return while improving safety, health and the environmental metrics for the facility.

A modular procedure consists of logical steps and as shown in Figure 3, each operator has started with the same SOP but has modified it to handle different situations and styles of operating by adding additional steps. On the right-hand side is the resultant "best-practice" procedure.

Milford Haven Revisited

Now let's revisit the Texaco Milford Haven refinery incident. In terms of a set of circumstances where the system could have potentially provided the operators with the correct information at the right time and possibly even taken corrective actions, this was a 'perfect storm'.

Texaco had a DCS, but while the technology didn't exist at that time to provide the kind of highly optimised HMIs that we have today, many things could have been done to reduce the operator mental workload and possibly have avoided the incident.

Alarm management could have reduced the number of high priority alarms so that those that activated were timely and did not overload the operator and if many activated at the same time, the system could have identified the possible 'main actor' enabling the operator to take action, or even taking action itself. For instance, the flare drum high alarm that was missed could have triggered a procedure.

These days we have better historians and data analysis tools, able to identify incidents as they start to occur and we can use intelligent displays to help the operator to see where the main activities need to take place.

Procedures should have been followed and the incident report recommended improved training and document keeping. But again today, a procedural assistant could give clear communications regarding;

- What was transpiring as the incident unfolded
- Next steps according to approved safety procedures
- Safety hazards associated with missteps

The incident report cited the inability of the operators to be able to carry out mass and volume balances. A procedure assistant could have helped with this and triggered actions or prompts as a result of an imbalance.

Can Standards Based Decision Support Help Mental Workload in a Crisis?

In the human factors section of the Texaco Milford Haven refinery incident report, one of the key factors mentioned was that the preparation of shift operators and supervisors for dealing with a sustained 'upset', and therefore stressful, situation was inadequate and that better overview facilities should have been provided.

This article has shown that issues often exist with humans in the workplace during times of crisis and stress. In some cases having the right human (or humans) in the right place can be beneficial – and often this is the case. But we need to be prepared for the situations where the operator gets overloaded or takes things for granted or when an inexperienced operator is working at the time things start to become unstable.

In times of abnormal operations, systems are configured to produce lots of data – humans are not configured to handle or interpret them. However, when presented with the right information, in the right context, during an abnormal condition, humans are able to do things machines cannot. They can evaluate the situation and provide the "thought process" on what action to take, with the guidance and support of automated systems.

> “Texaco had aDCS, but while the technology didn't exist at that time to provide the kind of highly optimised HMIs that we have today, many things could have been done to reduce the operator mental workload and possibly have avoided the incident.”