The operator as IPL

Author, User Centered Design Services, LLC, USA, looks at the role of the operator as part of an independent protection layer.

During the design of new plant, designers endeavour to minimise risk. However, the very nature of the process and the hazardous materials used in the processing requires the designers to reduce risks to an acceptable level by using multiple protection layers in an operating facility. These layers are known as 'independent protection layers' (IPLs).

The first layer is the process design and involves special process designs, process equipment, management systems such as procedures and training, and layouts. This layer has found new momentum in the Inherently Safer Design movement, which works on principles such as 'materials that are not there cannot leak'; removal of inter unit storage and storing less hazardous materials.

The second layer focuses on higher reliability and greater consequences in the event of failure of the basic process control system (BPCS), together with critical alarms, operator supervision and manual intervention. In recent years, operator supervision has declined and become more of an administrative function, while alarm management has become an Achilles heel to the protective layer. While manual intervention is often taken for granted, any failure is generally attributed to human error without attempting to resolve the root cause that promotes it. Emphasis is placed on other protection layers as this layer is uncomfortable for engineers who are more comfortable designing the physical layers or the automated safety instrumented system (SIS), and writing management systems for emergency response.

The next layer has even higher reliability but should require no operator intervention and is designed for automatic intervention. A lot of emphasis is placed on this third layer: the automatic SIS. This layer was developed before the programmable electronic systems (PES) technology and involved electromechanical relay based shutdown systems and/or pneumatic logic and interlocks. Today, it has been automated to a level that resembles an aeroplane's triple redundant protection system. It is clearly defined through standards, both local and international, and uses certified equipment, designs and in some countries, designers.

Other layers exist but they are generally physical, such as relief valves, containment dikes and management systems. These layers are well engineered and the industry has gained much experience standardising, implementing, operating and testing equipment and management systems within these protective layers.

Each of these independent protection layers work together to provide a unique solution and offers the designer alternative tools to meet the safety integrity levels (SILs) of a given process. These SILs are derived from analysis: 'The need to derive and associate SIL values with processes is driven by risk based safety analysis (RBSA). RBSA is the task of evaluating a process for safety risks, quantifying them, and subsequently categorising them as acceptable or unacceptable. Acceptable risks are those that can be morally, monetarily, or otherwise, justified.

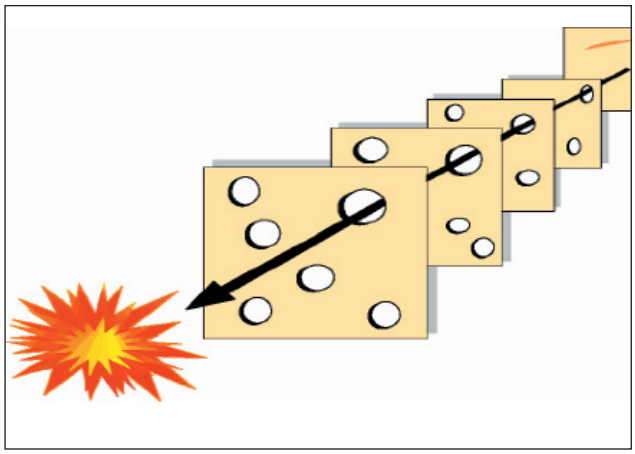

Figure 1. An accident trajectory passing through corresponding holes in the layers of defence, barriers and safeguards.

Conversely, unacceptable risks are those whose consequences are too large or costly. However risks are justified, the goal is to arrive at a safe process.'[1]

Operator intervention

As stated earlier, within each of the independent protection layers are multiple options and multiple layers for partial or full mitigation of the consequences of one potentially hazardous event (loss of containment, a fire, toxic release, etc.). However, it is interesting to note that AIChE CPPS Guidelines for Safe Automation for Chemical Processes states that 'the BPCS often functions as a protective layer, but this multipurpose instrument systems fails the test of specificity as the BPCS's first purpose is to regulate the process in day to day operation… Therefore, the BPCS should not generally be considered an IPL.'[2]

Many incident investigations have focused on the layer involving the BPCS, the supervisor, critical alarms and operator intervention as root cause for many incidents, but there has not been regulation or design focus for the other layers to resolve this problem. If the BPCS is not considered an IPL, the supervisor is not supervising, and the alarms are not functioning, then the IPL must then be left to operator intervention. This is highly variable due to the reliability of people and the factors that impact human performance.

Not claiming risk reduction from this layer may be acceptable; however, an event could have been prevented had this protection layer been effective. Experience shows that incidents happen when two or more safety barriers are broken as illustrated in James Reason's Swiss cheese model of accident trajectory (Figure 1), which indicates that active and latent failures can create gaps in the defence.

James Reason identified active and latent conditions as: 'Since people design, manufacture, operate, maintain and manage complex technological systems, it is hardly surprising that human decisions and actions are implicated in all organisational accidents. Human beings contribute to the breakdown of such systems in two ways. Most obvi-

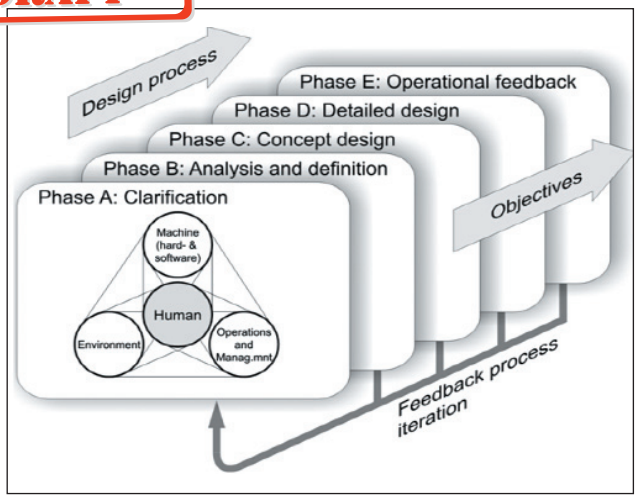

Figure 2. ISO 11064 Ergonomic Design of Control Centres.

ously, it is by errors and violations committed at the 'sharp end' of the system, by operators, maintenance personnel and the like. Such unsafe acts are likely to have a direct impact on the safety of the system and, because of the immediacy of their adverse effects; these acts are termed active failures…

Latent conditions are to technological organisations what resident pathogens are to the human body. Like pathogens, latent conditions, such as poor design, gaps in supervision, undetected manufacturing defects or maintenance failures, unworkable procedures, clumsy automation, shortfalls in training, less than adequate tools and equipment, may be present for many years before they combine with local circumstances and active failures to penetrate the system's many layers of defence.'[3]

Hence, people live with many of these conditions and suffer the consequences. Why? Part of the problem is due to the fact that engineers are more comfortable designing equipment and management systems than tackling human error. Most engineers have received very little information in the way of human factors and ergonomic training. Universities fail to find time in the curriculum for human factors and human error removal.

Techniques such as Human Reliability Analysis are foreign to operations personnel and management; hence, a problem has developed, as manifest in the major catastrophic accidents of Chernobyl, Piper Alpha and Bhopal.

The bottom line of most studies into human error indicates that human are more likely to make an error if they are:

- Required to make an important decision quickly under emergency conditions.
- Required to make multiple decisions in a short time span.
- Bored or complacent.
- Poorly trained in procedures.
- Physically or mentally incapable.
- Subjected to confusing or conflicting displays or data.
- Unqualified for their job.

Ergonomics indicates that, in order to minimise human error, the industries providing equipment, instrumentation and maintenance systems should recognise and address the following considerations in designs:

- Engineering console complexity.
- Access to information and information displays.
- Number of operator consoles per operator.
- Lighting requirements.
- Seating requirements[4].

This information has been available since the early 1990s in the Safe Automation Guidelines. Why have they not been adopted into what has been identified as an IPL and a recognised cause of previous failures?

One reason for non compliance is culture. Engineers and managers make cultures but they do not understand how to shape a culture or influence an existing culture to conform to these human error reduction techniques.

Each of these topics are addressed by the ISO 11064 Ergonomic Design of Control Centres; International Standard and CRIOP in Europe is a methodology that contributes to verification and validation of the ability of a control centre to safely and efficiently handle all modes of operations, including startup; normal operations; maintenance and revision maintenance; process disturbances; safety critical situations; and shutdown.

One of the most important principles of the CRIOP method is to verify that a focus is kept on important human factors, in relation to operation and handling of abnormal situations in offshore control centres, and to validate solutions and results. Key principles in human factors design are:

- Improve design through iteration (Figures 1 and 2, adapted from ISO 11064).
- Conduct human factors analyses such as function and task analysis.
- Ensure systematic end user participation.
- Form an interdisciplinary team.
- Document the process[5].

The following are attempts to address each of the recommendations.

Making an important decision quickly under emergency conditions

A model has been produced of operator decision making and success and failure outcomes. The key to success in this area is good orientation of an event through well managed alarms, clear hierarchical graphic navigation that allow the operator to evaluate the problem, and finally collaborative actions with training and procedures.

To address this issue, many plants have used training and procedures to equip the operator for these situations. They practice decision making and initial response without a procedure by rehearsal, and if available, doing drills with simulators, tying training and procedure practice to these scenarios.

Some companies have added technology to allow the production process to be dramatically reduced or recirculated. The technique uses either automated or semiautomated interactive procedures and it models important equipment to ensure safe, reliable operation.

Operators are also prepared for this event through diagnostic decision making training courses and team building exercises.

Making multiple decisions in a short time span

Keeping track of actions or information is a challenge to humans as they can only memorise three pieces of information in short term memory during fast moving or stress related events. Companies are providing tools at the console to allow the operator to offload some of these memory tasks. Operator alerts are one technique that is used to transfer reminders from memory to the automation system. An example is 'drain valve is open and should be closed before startup'.

To address this issue, many organisations have used training and procedures to equip the operator for abnormal situations. They practice the decision making and initial response without a procedure by rehearsal, and if available, doing drills with simulators, tying training and procedure practice to these scenarios.

Boredom and complacency

Due to the evolution of jobs, some stations are overloaded and many are under loaded. This causes boredom and complacency. In the past, managers did not have a good technique for measuring workload. Time and motion studies were all that were available. These became very subjective as similar processes were deemed to be different, based on a single maintenance event rather than a long term perspective.

Today, new techniques for measuring console and field operator workload are available. These are based on equipment count; equipment complexity and additional workload for operators based on interactions between units or separation by intermediate storage vessels; DCS workload implied by over alarming; poor graphics and navigation; the integrity of the control system; and its performance for maintaining automatic control.

Through job design and job performance profiles, boredom and complacency is being removed.

Poor training in procedures

Today, companies that capture the vision of operational excellence and production centred organisation place different priorities on operator and supervisory training. They invest in subject matter experts to prepare material and 'trained' trainers to deliver the training. They are cautious about how much and how the mentoring and on the job training is done. They focus on consistency.

Procedures are often up to date to OSHA PSM standards but are useless for many situations and are unused by operators. Scenario based training with procedures continuously enhance and make procedures more usable. Operators are expected to know the first 20 steps in emergency procedures and should know where to find a current copy of a procedure. Important procedures will always be followed and a checklist will be signed off for each step. Supervision monitoring procedure progress and identifying potential problems by being intimately involved in the delivery of the procedure are also proving valuable.

Physical or mental incapability

There are tremendous challenges with 12 hour shifts and the extra hours worked in overtime by operators. Fatigue, sleep deprivation and illness are all potential problems that the shift worker faces. A formal work related stress programme and fatigue countermeasures should be enforced.

Work related stress can be defined as the adverse reaction people have to excessive pressure or other demand placed on them. The Health and Safety Executive in the UK observes the consequences that work related stress can cause for organisations[6], including:

- An increase in sickness absence, which can have a domino effect; one person is off sick, which leads to their workload being shared among the remaining staff. They in turn may then be unable to cope, which could affect their health and further sickness absences.
- Reduced staff morale.
- Reduced staff performance.
- Staff seeking alternative employment. Organisations then have the expense of recruiting, inducting and training new members of staff.

Most of the 'things to do' boil down to good management. They are ongoing processes that need to be built into the way an organisation is run:

- Show that stress is taken seriously and be understanding towards people who admit to being under too much pressure.
- Encourage managers to have an open and understanding attitude to what people say to them about the pressures of their work, and to look for signs of stress in their staff.
- Ensure that staff have the skills, training and resources they need so that they know what to do, are confident that they can do it and receive credit for it.
- If possible, provide some scope for variety in working conditions and flexibility. Allow people to influence the way their jobs are done. This will increase their interest and sense of ownership.
- Ensure that people are treated fairly and consistently and that bullying and harassment are not tolerated.
- Encourage good two way communication, especially at times of change.

A number of different programmes are available to address fatigue; the simplest is the introduction of exercise equipment for shift console (process control) operators who do not get outside the control room. Some operators do not like taking exercise so they should be encouraged to take regular short breaks. Operators benefit little from circadian lighting systems but greatly from nap rooms which, if managed correctly, can mean the difference between an operator performing to expectations or missing an important event that could be catastrophic.

Confusing or conflicting displays and data

Most P&ID designed graphics on DCS displays are overcrowded. The text is too small and often overwritten. The overuse of colours and using the same bright intensity makes identification of change difficult. This produces poor situation awareness and causes fatigue and eye strain. Alarm systems that are out of the EEMUA 191 performance metrics burden an operator and cause confusion, missed events and break the diagnostic model by not orienting the operator correctly or providing prioritisation to multiple tasks. A number of major catastrophic accidents have identified the human computer interface (HCI) and the alarm management system, in particular, as contributing causes to the event, confusing operators and introducing human error.

Under qualification

In the past few years, companies have moved toward dedicated positions, and the technical skills required for these new job profiles have been significantly enhanced. This is true for the console operator and the field operations. In the control room there has been a significant move towards advanced process control, unit and plant optimisation practices, which requires the operator to be more proactive to keep the basic regulatory control working to its best possible performance and manage the advanced control to keep the process within constraints.

The field position has been enhanced by autonomous maintenance practices and operators are taking more responsibility for given assets. This new role involves more measurement and tracking of key performance indicators (KPIs).

User Centered Design Services has identified a best practice for console operators to maintain proficiency in the

field positions. A realistic rotation is developed based on shift patterns and minimum time to maintain a level of competence in any job position.

Engineering console complexity

The HCI impacts the operator's performance and ability to identify or orientate the operator to changing situations. However, it is not just the graphics themselves. It involves navigation, the ability to keep the big picture but still drill down into detailed information and supporting diagnostic data. This delivery of information and data is supported by the console design, the number of DCS graphic screens, usage of overview displays, and how the operator interfaces with the system using keyboards, mouse, trackball and displays. The workstation needs to accommodate the ability for the operator to use paper, from simple notes and memos to detailed design documents, procedures and P&ID drawings.

The console is also the main communication centre for internal and external communications and should be designed for clear and disturbance free communication and collaboration. This means segregation from other distractions such as alarm horns from other units, radio traffic and people moving around the control room.

The ISO 11064 standard demonstrates how to design and layout consoles for good ergonomics that support good communication and collaboration.

Access to information and information displays

It is important during a plant disturbance that the operator is allowed to work through diagnostic routines without disruption; however, it is equally important that managers, engineers and supervisors have access to information without disturbing the operator. Many control rooms employ a 'war room' concept where they can meet talk and view information and be close to the operator to provide guidance.

The operator's direct supervisor or support staff must also have access to terminals adjacent to the console operator but again without breaking the operator's attention. User Centered Design Services recommends a dedicated supervisor console that can view any graphic from any console in the control room. Application development engineers should also have access to workstations in the control room and recommend a dedicated development area with a near adjacency to the control room.

Number of operator consoles per operator

Having the right number of operators is more than counting control loops or a manager's educated guess. Today, control rooms are staffed based on a model. This includes equipment count, equipment complexity, equipment connections to other units (feed and stock) and the DCS added workload that may be due to alarm management problems, poor graphics navigation, loop integrity and how many moves an operator makes.

A staffing model provides a number of console operators; the information then confirms each individual operator's scope of control, which in turn is used to determine the number of screens on a console per operator and the size of the console.

The designer needs to determine whether one operator can manage a disturbance, the number of operators required for a plant shutdown or startup and, if additional operators are required, whether they will be required in the control room or a local control house if separate.

In some cases, an extra operator position will be provided at the control console. Effective improvement to communication can be observed by bringing an extra console operator into a field shelter with field operators, and allowing this extra person to startup equipment while in face to face communication with the field operators, and unit to unit communication being done in the centralised control room (CCR).

Lighting requirements

Since the addition of DCS control, little attention has been paid to human factors and ergonomics, resulting in the implementation of HCIs that are overly colourful and that use poor intensity or too bright hues against black backgrounds. This causes high contrast and major glare issues. Operators tend to run consoles with control room lighting either very low or off, but this is a poor solution as it causes fatigue and problems with adjusting to shift rotations and night work. Circadian rhythms are difficult to synchronise with older workers. Operators found it difficult to read text with these lighting levels, causing problems when using multikeyboards due to difficulties reading the keyboard text.

Instead, the industry has switched to using low intensity or very limited colours against grey backgrounds, thus allowing control room lighting to be raised to office levels of approximately 500 LUX. This is a better work environment and reduces many areas of stress related problems.

Operators who are used to dark control rooms may be reluctant to turn the lights on even though they have the new HCI with grey backgrounds, and lighter displays in dark rooms can cause new problems. The reluctance to turn the lights on may be because it was easier for management to catch employees napping, thus leading to discipline. Operators should not be disciplined for accidental napping but rather for deliberate sleeping or making a bed.

Seating requirements

Many managers have a problem investing in good computer chairs for operators and the result is broken, poor ergonomic chairs that are unsuitable for 24 hr operation. The investment in good quality, lifetime warranty chairs is a much better investment than having rooms full of broken and badly repaired chairs.

Good ergonomics are important because they impact the alertness and performance of the operator. It also reduces risk of work related stress, causes of stress and physical repetitive stress injuries.

Conclusion

These items may not be the full story from a human factors expert and may not have gone through full human error reduction, but from identified incidents, will reduce some common causes. If the combination of BPCS, critical alarms, supervisors and operator intervention are an important risk reduction method and part of an independent protection layer, a better solution should be provided. Resolving the alarm management issues and providing adequate supervision should be a priority.

References

1. Application Note: Bentley Nevada - Functional Safety and Safety Integrity Levels.
2. Guidelines for Safe Automation of Chemical Processes, CCPS p 16 footnote 1. ISBN 0-8169-0554-1.
3. REASON, James, Managing the Risks of Organizational Accidents p 10. ISBN 1-84014-105-0 Ashgate Publishing Ltd.
4. Guidelines for Safe Automation of Chemical Processes, CCPS page 66 ISBN 0-8169-0554-1.
5. CRIOP report produced by SINTEF.
6. Health and Safety Executive, Management Standards for Tracking Work Related Stress, 'The Management Standards'.