OPERATOR EFFECTIVENESS BY DESIGN

Robert A Weiss[1]
[1]Honeywell Process Solutions
679 Victoria St, Abbotsford, Victoria 3067, Australia
bob.weiss@honeywell.com

ABSTRACT

Effective operator responses to deviations in process operation are critical to plant safety and profitability. However, designing operator effectiveness into a greenfields plant has proved challenging. Focusing on the role of the control room operator, this paper discusses the elements of operator effectiveness, the barriers to achieving this during the normal design process and a process that overcomes these challenges.

Large centralised control systems are intended to maximise operator situational awareness, but often have the contrary effect. Excessive alarm loading, absence of an effective process overview and excessive operator distractions are common problems. Guidelines developed by the Abnormal Situation Management Consortium and EEMUA in the UK have been successfully applied on many existing facilities and can lead to substantial improvements. For example, one study identified savings from more effective display design of about A$1M p.a.

However, applying these principles when a plant does not yet exist can prove problematic. When designing a new facility, operating experience is not available for guidance, and the contractual process can be challenging. For example, the work of diverse subcontractors can often result in unintended high operator console alarm loading. Effective handover from design to operations can also be difficult.

To build in operator effectiveness from the outset, the operating company must “own” the process throughout the project. Based on the author’s experience, an effective design and implementation process that helps ensure operator effectiveness is presented. The paper also briefly discusses the emerging role of operator training simulators for confirming operator effectiveness prior to commissioning.

INTRODUCTION

Effective interaction of the control room operator with the control system is critical to successful performance of major process facilities. In particular, the effectiveness with which operators intervene to manage so-called “abnormal situations[1]” is critically dependent on how well their mental model of the current situation matches reality (Cochran 1997). Figure 1 below shows a typical cognitive model used to better understand operator intervention. Intervention becomes ineffective if either of the two feedback loops is interrupted or provides erroneous information.

---

[1] An abnormal situation occurs when automated control system action is no longer effective, and operator intervention is required to restore normal process operation.

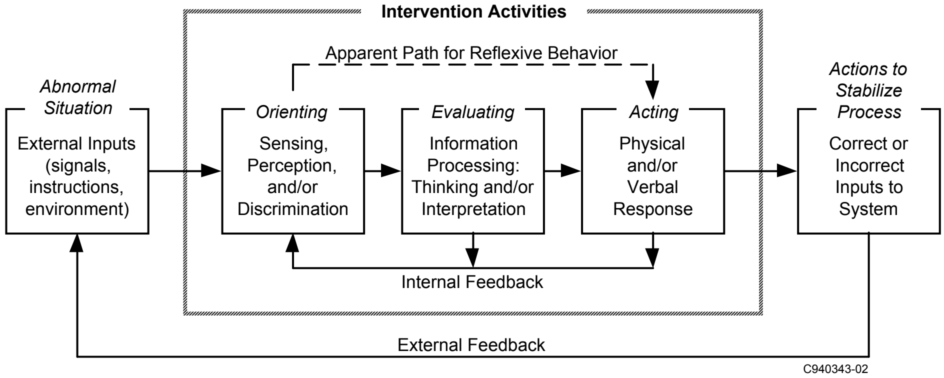

Figure 1: Standard model of human interaction with complex systems. (Cochran 1997)

Examples of major accidents where mismatches in understanding caused by erroneous feedback of process state contributed to the causal chain are the fire at the Texaco Milford Haven Refinery in 1994 (HSE, 1997) and more recently the explosion and fire at the Texas City refinery (CSB, 2007). Given that the principal source of the control room operators' understanding of the process state is the control system Human Machine Interface (HMI), the design, implementation and maintenance of the HMI is critical to operator effectiveness.

The Abnormal Situation Management Consortium, a research consortium founded in 1994, has developed techniques and guidelines to maximise the effectiveness of the control room operator. As well as aspects of the control system HMI design, such as displays, alarms and console layout, they also cover the other aspects of the control room operators' environment. These include control building design, procedures, training and effective operational communications. These techniques have been successfully applied to both existing and new facilities. This paper focuses on two important aspects of the HMI design that impact operator effectiveness - alarm system design and display design.

ALARM SYSTEM DESIGN AND MANAGEMENT

Computer-based control systems such as DCS and SCADA systems provide alarms "for free". Alarms are therefore often seen as not warranting design effort. Moreover, many process engineers consider that unless an alarm is provided, the operator will not respond. This philosophy is embodied in specifications from major engineering contractors that effectively require an alarm to be applied for every possible deviation. It is therefore not surprising that the number of alarms on a typical process plant escalated from hundreds to thousands over the 1990s (Andow, 2000). The discipline of engineering individual alarms has largely been lost. The result is that the alarm system often fights the operators rather than supports them.

To address this, research from the ASM Consortium and the UK HSE was published in the 1999 EEMUA Publication 191, *Alarm Systems, A Guide to Design, Management and Procurement*. The second edition was released in 2007 (EEMUA 2007). This provides guidance for the design, ongoing improvement and management of alarm systems. In particular, it establishes benchmarks for alarm performance. The number of standing and shelved alarms and the average and peak alarm rates over a period are important indicators of alarm system performance. Typically these are used to guide an improvement program on an existing facility. Figure 2 shows one successful approach.

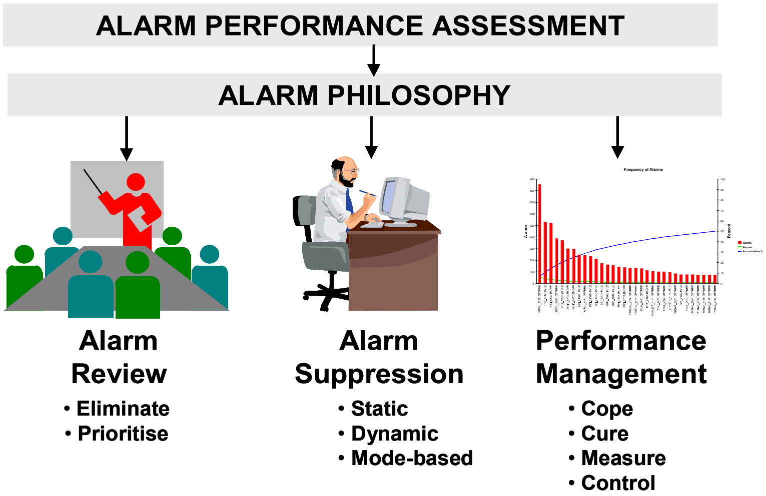

Figure 2: Components of an alarm improvement program (Weiss 2005)

In summary, the process used is as follows:

1. For existing facilities, carry out an assessment of current alarm system performance. Use this to establish a benchmark, to identify which level of maturity applies and diagnose specific corrective action.
2. Prepare an Alarm Philosophy defining the fundamental criteria for alarm system design, management and operation. This is an essential requirement for all facilities. A workshop facilitated by a specialist can be a powerful way of gaining commitment by all parties whilst developing the key bullet points for the alarm philosophy.
3. Based on the Alarm Performance Assessment and the Alarm Philosophy, determine the appropriate mix and sequence of the remaining three activities that are intended to get the alarm system performance from that measured by the Alarm Performance Assessment to the state embodied in the Alarm Philosophy.
4. Review each alarm in turn against the alarm philosophy to eliminate redundant alarms, set alarm priorities, document the basis for and response to alarms and verify alarm settings.
5. Set up ongoing management processes and software to monitor alarm system performance, enable the operators to cope with nuisance alarms, ensure the root causes of nuisance alarms are addressed and ensure that changes to the alarm system are controlled.
6. Selectively implement alarm suppression and other advanced alarm handling to the extent necessary to achieve the target alarm performance.

This process was originally developed to improve existing alarm systems on operating facilities. Modified versions have been used for the design of new facilities. However, the improvement process uses alarm system performance measurement as a key driver. This is not available for an alarm system during design. It also relies heavily on the experience of process operators, which is typically also unavailable or limited during design of new facilities. The process required is therefore somewhat different, and will be described below.

DISPLAY DESIGN

The second major aspect of control system design that impacts operator effectiveness is the design of the displays with which the operator interacts. Considerable attention is often given to this during detailed design. With careful design using a human factors-based approach, significant benefits can be realised. One study (Errington et al 2005a and 2005b) reported savings of $1M per annum. However, more commonly the end results are unsatisfactory. In particular, in the author's experience the operator's ability to obtain an effective overview of the process status and their ability to quickly detect abnormal situations are often suboptimal. Figure 3 compares a conventional display for a flotation process and one designed using human factors principles endorsed by the ASM consortium. Both displays contain essentially the same information.

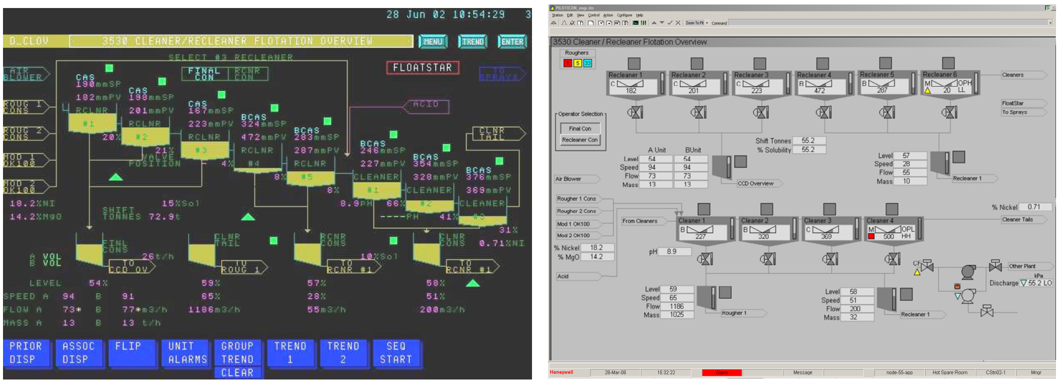

Figure 3: Conventional display (left) and equivalent ASM-compliant display (right)

Whilst it has been long recognised that it is important to involve the process operators in the design of process displays, the mechanism for doing so is often ad hoc and unsatisfactory. Operators know the process, should have a good feel for their requirements and have a good understanding of their existing or past HMIs, but they typically have minimal understanding of human factors principles and of the capabilities and limitations of modern HMIs.

The following display design process used on facility upgrade projects has been found to be effective at integrating operator experience with sound human factors.

1. Determine what tasks the console operator needs to perform, together with their approximate frequency (daily, weekly, a few times a year, rarely) and criticality. Important tasks to include are both casual and systematic process surveillance. The rigour with which this task analysis is performed can range from a full structured task analysis by a trained human factors professional through to simply interviewing operators from each shift. A facilitated workshop involving experienced operators, supervisors and control engineers can be very effective.

2. Determine the displays required to support each of these tasks. Where the requirements are similar, a single display can support multiple tasks. All common tasks and all critical tasks should be supported by a display. In particular, overview displays must be provided to support plant surveillance. However, infrequent and non-critical tasks do not necessarily require a specific display; some judgement is required.
3. For each task identify what information and interaction are required on each display. It is helpful to use existing displays as a checklist – which of the current display items are required which are not, what are missing, how can interaction be improved etc. For many process plants, overview displays are often best provided by trends, perhaps in conjunction with some other indicators.
4. Determine the "hierarchy of salience" for display elements. Which need to be most prominent? Typically the highest priority alarms. Which need to be least prominent? Typically tag numbers and equipment IDs.
5. Develop standards for each display element to achieve the appropriate salience hierarchy under the proposed control room lighting. A bright lighting level similar to normal office lighting (500-1000 lux) is preferred to maintain operator vigilance. However, if some traditional displays with a dark background are to be retained, lower lighting levels will be required to achieve the necessary display contrast. Trial various combinations of colours and shapes using the target HMI hardware and lighting. To ensure acceptance, it is essential that operators are involved in this process as the results can be surprising.
6. Decide the best way to display and interact with each element. Use a shape library to ensure consistency. Complex objects such as embedded trends and filtered alarm lists can greatly enhance usability, but are often overlooked.
7. Develop effective standards for navigation between displays. First identify the primary purpose of each screen in a cluster. Consider also where pop-up displays should appear and how to direct displays to particular screens. Organise displays in a well-structured hierarchy with consistent navigation.
8. Prototype at least one typical display of each type, implementing sufficient numbers to test the navigation scheme proposed as well as the individual display content. Arrange adequate review by operators from every shift, ensuring that the underlying principles have first been adequately explained. A workshop environment is very helpful for this. Nevertheless, it is essential that all users feel they have an opportunity to contribute, even though it is usually not possible for all to attend workshops, or to adopt all their ideas. Explaining the rationale behind each decision is important to help build acceptance.
9. Capture the final agreed requirements in a brief display philosophy that summarises the principles, as well as a display standard that defines the implementation details in terms the control system engineers can directly apply.
10. Design, implement and deploy the remainder of the displays in accordance with the standard, ensuring adequate detailed operator review and testing.

Alternative approaches are possible, but the approach used must ensure that experienced operators are involved and employ sound human factors principles.

GREENFIELDS PROJECTS

A project to design, construct and commission a greenfields facility represents the opposite extreme to an on-site operational improvement project. Many projects require some combination of these two approaches.

A typical greenfields project involves the following parties:

1. The end-user operating company for whom the facility is being built. They have responsibility for specifying requirements, engaging the major contractors to execute the project, commissioning and ongoing operation of the new facility.
2. A design contractor that performs the front end engineering design (FEED).
3. An engineering, procurement, and construction (EPC) contractor that performs the detailed design, procures the necessary equipment and services and constructs the facility.
4. A control systems vendor that supplies and usually implements the process control system. This often includes configuring all alarms and detailed design and configuration of the operating displays. Traditionally, the control systems vendor would be contracted by the EPC contractor. More recently it is becoming common for the operating company to partner directly with the system vendor.

Under usual contractual arrangements, those implementing the alarms and displays can be a long way removed organisationally from the process operators who will ultimately use the HMI. The previous sections have indicated the importance of effective operator involvement in HMI design. This does not occur naturally under traditional turnkey EPC contracts. Moreover, neither the typical EPC contractor nor the control system vendor has sufficient detailed knowledge by themselves of how the process will be operated to develop an effective HMI. Also, the budget and schedule may not recognise the interactions and iteration required for effective HMI design. In particular, appropriately experienced operators may not be available sufficiently early in the project.

A common practice is for the EPC to pass a set of P&IDs to the control system vendor and request a display to be developed for each P&ID. Similarly, all so-called alarms specified by process engineers and package vendors are passed through to the control system vendor uncritically for implementation. Although efficient, these processes invariably result in a very poor operating environment. On major facilities, alarm performance will typically exceed the "Level 1 Overloaded" alarm regime (EEMUA 2007, Fig 7). On one new facility, losses of several hundred thousand dollars occurred because the operator lacked an appropriate overview of process operation, and important alarms were buried in the 1400 standing alarms.

The key challenges in developing an HMI on a greenfields project include:

1. Ensuring commitment to operator effectiveness from the operating organisation right from the start of the project, and clear ownership at each phase of the project.
2. Marshalling and co-ordinating appropriate expertise from the operating company, EPC contractor and control system vendor.
3. Making available suitably experienced operations personnel early in the project.
4. Recognising and complying with the realities of the project schedule.
5. Ensuring that requirements for the alarm system and HMI are specified explicitly to the engineers responsible for different aspects of the design.
6. Influencing the design and managing inputs (particularly for alarms) from many diverse sources, particularly the package equipment vendors.
7. Ensuring that default control system alarm settings are appropriately adjusted
8. Understanding that the alarm system design will not be perfect and some commissioning adjustments will be required.

Unlike the improvement processes discussed above, no performance data is available to guide improvements. Operating experience is also non-existent with the new facility and instead is gained from similar facilities. Process knowledge rests primarily with process engineers rather than operators. This changes the approach required somewhat. An ineffective HMI rarely results from technical limitations, but rather from inadequate management of the diverse parties involved, and lack of understanding of human factors design. An approach that addresses the above challenges is discussed below.

Overall responsibility for the effectiveness of the control system HMI cannot be subcontracted. Some elements of ensuring the effectiveness of the HMI are clearly the responsibility of the EPC contractor and the control system vendor. However, the operating organisation is involved from project conception to operation, determines the facility operating philosophy and appoints the operations team. These factors have an important influence on the ultimate success of the alarm system and the HMI.

As operating companies realise the criticality of the process control system to ongoing operations, some are forming a partnership with a control system vendor early in a greenfields project. This facilitates transfer of knowledge between both parties. Although this is a great improvement over a traditional adversarial contractual arrangement, a structured process is still required to ensure success.

The following approach is recommended.

1. At the start of the project, appoint an individual with responsibility for ensuring the control system is engineered to maximise operator effectiveness. Ideally this should be a senior operations representative, but is often the operating company's lead control system engineer. They must ensure appropriate contractual clauses are in place, make available experienced operators for input

to the HMI and alarm design and ensure effective continuity between the project, commissioning and operation phases.

2. Prepare a concise alarm philosophy and display design philosophy early in the project. These documents must state the “basis of design” for the alarm system and control system displays. They should be limited to the principles to be followed and be concise. They must include input from experienced operators. Ideally these documents should be prepared by the operating company prior to the Front End Engineering Design (FEED) phase. Alternatively they can be prepared early in the FEED process. They can be incorporated in the Basis of Design for the Process Control System, or could be standalone documents. In either case the contents must be owned and believed in by the operating company. Development via a philosophy workshop can be effective if appropriately experienced people are available.
3. During the FEED, the principles in the two philosophy documents must be developed into design specifications. They must specify both “what to alarm” and “how to alarm”. It is critical to success that these specifications recognise that “what to alarm” is NOT primarily the responsibility of the control systems engineer. Process engineers, package equipment vendors and other subcontractors specify alarm requirements. These parties will not see the control system detailed specification. The appropriate requirements must be promulgated in the relevant specifications suitable for each audience. “How to alarm” and display configuration standards can be part of the control system detailed specification, or separate documents. An adaptation of the workshop approach discussed in Alarm System Design and Management and Display Design above can be used to develop these specifications. This must include prototyping of displays and navigation schemes for review by operations representatives. Timing depends on access to a senior operator but details need to be finalised relatively early during detailed design.
4. Those responsible for specifying what to alarm should then comply with the relevant specifications.
5. Late in FEED or in early detailed design an alarm review should be held. This is similar to an alarm review on an existing facility but does not review alarm settings and must review all alarms. Subsequent alarm reviews will usually be required for packaged equipment as the information becomes available. Packaged equipment normally causes more problems than the core process design. Alarm configuration metrics (see EEMUA 2007 Tables 15 and 25) should be progressively checked to avoid excessive numbers of alarms.
6. Late in FEED or in early detailed design the design contractor should work with the control system vendor to specify default alarm settings as part of specifying standard control block and other control system configuration. Operator input should be sought as appropriate. Those alarm parameters to be determined in alarm reviews should be explicitly identified. All manufacturer default alarm settings must be reviewed and replaced as necessary prior to configuration starting.

7. During detailed design, alarms are configured as data becomes available.
8. During detailed design, displays are implemented in accordance with the specification. An operator review cycle must be incorporated. Displays must be completed and thoroughly tested as part of Factory Acceptance Testing. Use during operator training, particularly with an operator training simulator, can identify necessary changes required prior to commissioning.
9. Prior to final process commissioning, the tools and processes for ongoing alarm system management must be established and commissioned.
10. Just prior to control system site commissioning, a brief audit of alarm review actions and status should be undertaken. This identifies any outstanding actions that need to be completed.
11. During commissioning, alarm settings (particularly deadbands and time delays to avoid chattering alarms) should be reviewed and adjusted as appropriate.
12. During early operation a simplified alarm review should be undertaken to remove redundant alarms, review settings and audit the ongoing process for alarm system management. If the previous steps have been conscientiously followed, changes required should be minor.

The above process provides a sound basis for ensuring that as far as possible the commissioned control system will maximise operator effectiveness whilst also meeting project objectives. Nevertheless, further improvements should be possible using operator training simulators.

A FUTURE ROLE FOR OPERATOR TRAINING SIMULATORS

As high fidelity operator training simulators have become more affordable, their use on major greenfields process plants is becoming commonplace. Although their primary role is to accelerate operator training, recent experience shows that simulators often pay for themselves just by detecting process design and control issues prior to commissioning. As modern simulators use the actual control system HMI, during operator training the simulator is also often used informally to identify issues with operating displays.

Extending this role by undertaking more structured usability assessments during design should lead to significant benefits in display design. For example, Nova Chemicals undertook a highly structured assessment using simulators in 2004 following commissioning of their new ethylene plant (Errington et al 2005). It should also be possible to use the simulator to obtain an initial assessment of alarm system performance, and make some improvements prior to commissioning. So far, however, success in this area has been limited. This is because the time available for simulator implementation is sandwiched between finalisation of control system configuration and testing and the start of operator training. This typically leaves no additional time for structured reviews or performance assessments. To overcome this in the future, more explicit planning is required, together with use of non-invasive review techniques for the HMI and alarm system during operator training sessions. Together with the techniques outlined above, this should allow a significant improvement in operator effectiveness on major greenfields projects.

REFERENCES

Andow, P 2000 ‘Alarm Performance Improvement During Abnormal Situations’, *Hazards XV: The Process, Its Safety, and the Environment: Getting It Right*, Institution of Chemical Engineers, Manchester, UK, 2000

Cochran, EL 1997 *Managing Abnormal Situations in the Process Industries I: Automation, People, Culture,* viewed 10 May 2008, < http://www.asmconsortium.com>

CSB 2007, *Investigation Report, Refinery Explosion and Fire, BP Texas City, Texas, March 23 2005,* Report No. 2005-04-I-TX, March 2007 U.S. Chemical Safety and Hazard Investigation Board, viewed 10 May 2008, <http://www.csb.gov/completed_investigations/docs/CSBFinalReportBP.pdf>

EEMUA 2007, *Alarm Systems: A Guide to Design Management and Procurement. 2nd Ed. Publication 191,* 2007 The Engineering Equipment and Materials Users Association, 45 Beech Street, London EC2Y 8AD. www.eemua.co.uk

Errington, J et al, 2005a ‘Establishing Human Performance Improvements and Economic Benefit for a Human-Centered Operator Interface: An Industrial Evaluation’, *Proceedings of the Human Factors and Ergonomics Society 49th Annual Meeting*, Orlando, FL, 26-30 September 2005, viewed 10 May 2008, <http://www.asmconsortium.com>

Errington, J et al, 2005b, *Supporting Key Console Operator Interactions through the Control System Interface*, 17th Annual Ethylene Producers’ Conference, Atlanta, Georgia, April 10-14, 2005, viewed 10 May 2008, <http://www.asmconsortium.com>

HSE 1997. *The explosion and fires at Texaco Refinery, Milford Haven, 24 July 1994*. Health and Safety Executive, Her Majesty’s Stationery Office, St Clement’s House, 2-16 Colegate Norwich NR3 1BQ.

Weiss RA, 2005, *Taming your Alarm System - Experience from the Field,* IICA National Symposium, Melbourne, Australia, September 2005.

BRIEF BIOGRAPHY OF PRESENTER

After 7 years with Monsanto as a process engineer and production supervisor, Bob Weiss spent 18 years with ICI Engineering, for much of this time leading a group responsible for process control, safety instrumented systems and manufacturing information systems on many of ICI Australia’s major projects. He was also a technical investigator for the Royal Commission into the 1998 Longford gas plant explosion and fire. As a consultant with Honeywell Process Solutions since 1999, Bob has assisted many major process operating companies both in Australia and overseas improve their alarm systems, develop effective ASM-compliant display standards and comply with functional safety standards. He is a Fellow of the Institution of Chemical Engineers and is both a Certified Functional Safety Expert and a TÜV Functional Safety Expert.