

“Better Alarm Management” by A G Foord & R V Lord

1. What is the problem?

In 1999 the Engineering Equipment & Materials Users Association (EEMUA) published the Alarm Systems Guide [EEMUA 1999] developed by members of EEMUA (including BP Chemicals). In early 2000, together with staff from 4-sight Consulting, EEMUA produced a one-day training course based on the Guide which has been run nine times to date. This article reviews the background to the need for the Guide, the main features of the Guide and the experience to date of implementing the Guide.

Alarms are intended to alert the operator, inform the operator that some action is needed and guide the operator to the appropriate action. Unfortunately the result is not always what was intended.

1.1. *Major Incidents*

[EEMUA 1999] and [HSE 1999] give many examples over two decades to illustrate the seriousness of the problem of controlling major incidents. A few examples where alarm management was one of the factors are summarised briefly here.

1.1.1. Three Mile Island - 1979

Operators failed to recognise that a valve was stuck open and this seriously damaged the core of a nuclear reactor. Poor design of the control panel, the distraction of a hundred alarms, inadequate operator training and a failure to remedy previous maintenance failures all contributed to the incident.

1.1.2. Union Carbide, Bhopal – 1984

A cloud of toxic gas killed over two and a half thousand people and affected a quarter of the city's population. A combination of incorrect operation, poor maintenance, failed alarm and safety systems and inadequate safety management allowed a dangerous chemical reaction to occur.

1.1.3. Herald of Free Enterprise – 1987

When a roll-on roll-off ferry sank rapidly in shallow water one hundred and eighty nine passengers and crew died. The pressure to achieve operational goals, the flawed safety culture, friction between ship and shore management, and the absence of an effective alarm or reporting system meant that the ship sailed with the bow doors open.

1.1.4. Texaco Refinery, Milford Haven – 1994

An explosion and the resulting fires at an oil refinery [HSE 1997] injured twenty-six people (none seriously) and caused £48M of damage plus major production loss. The pressure to keep operating, the lack of a process overview, the distraction of hundreds of alarms, and modifications that had not been fully assessed all resulted in an overflow of boiling, flammable liquid from the flare drum. Recommendation 6 of the investigation report [HSE 1997] states “The use and configuration of alarms should be such that:

safety critical alarms, including those for flare systems, are distinguishable from other operational alarms; alarms are limited to the number that an operator can effectively monitor; and ultimate plant safety should not rely on operator response to a control system alarm.”

1.1.5. Channel Tunnel Fire – 1996

Smoke from a fire that resulted in £200M of damage and lost revenue affected a number of passengers and some suffered shock. Previous problems with false alarms, the pressure to keep operating, and an overload of information, alarms and actions required by staff all contributed to delays in staff taking emergency actions. The inquiry report recommended that Eurotunnel install an alarm management system [CTSA 1997].

1.2. *Increasing demands for control*

Demands on operators are increasing annually because of:

- The need for operation close to maximum efficiency;
- Higher costs of process interruptions (for example the removal of intermediate or buffer storage);

“Better Alarm Management” by A G Foord & R V Lord

- More complex processes are now possible;
- Lower safety margins giving less opportunity to recover from upsets;
- Environmental regulation may mean simple venting to atmosphere or direct discharge to waterways or landfill may no longer be acceptable;
- Fewer operators;
- Higher staff turnover resulting in less experienced operators.

1.3. Increasing sophistication of control systems and processes

Thus to meet these increasing demands for control, more and more systems are operated by complex computer control systems. The role of the operator changes depending on the state of the system.

Operational state	Operator's primary role	Key alarm information
Normal	Monitoring & optimisation	Minor operating adjustments needed
Upset	Situation management	Operator intervention needed
Shut-down	Ensure safe shut down	Safety actions needed

But, more significantly, it is increasingly difficult for any one operator to understand both the complete process and the operation of the computer control system.

1.4. Neglect of Human Factors

The flaws in the “BE CAREFUL!” approach are well recognised, but ignorance of human factors is widespread. There has been a particular lack of understanding of how alarms can contribute to or distract from safe operation. This has resulted in many control systems that include thousands of individual alarms and an unspecified number of combinations of alarms. [HSG 1999] includes a formal definition of “human factors” based on the task, the individual and the organisation. Another way of viewing this is to avoid:

- Designing for oneself
- Designing for the average operator
- Trusting to common sense
- Unduly relying on operators for safety

1.4.1. Causes of human failure.

The major incidents described in [EEMUA 1999] and [HSE 1999] cover the full range of human failures:

1. Errors and mistakes
 - a) Skill based errors such as taking action not as planned or omitting an action – for example, not completely closing the bow doors on a roll-on, roll-off ferry.
 - b) Mistakes such as rule based mistakes when using a rule that no longer applies or knowledge based mistakes when the correct measurements are lacking or the operator is too inexperienced to reason correctly from the measurements – for example, not recognising that an alarm is safety related and needs immediate action.
2. Deliberate violations
 - a) Routine violations to save time or energy, or arising from poor training or poor supervision, or misconceptions about the value or applicability of the rules – for example, not recognising the need to close a facility and evacuate as soon as a fire is detected; or suppressing a repeating or erroneous alarm without following the correct procedure for alarm suppression.
 - b) Situational violations where the rule is difficult to apply, conflicts with other rules, resources are lacking or extreme conditions prevail – for example, trying to rely solely on control room measurements to avoid going outside in bad weather; or ignoring a safety related alarm while dealing with other alarms.
 - c) Exceptional violations where something has already gone wrong which leads operators to justify breaking a rule – for example, using unsafe short-cuts to recover normal operation when equipment has failed; or ignoring all alarms during alarm overloads.

“Better Alarm Management” by A G Foord & R V Lord

Good design of alarm systems can contribute to reducing all these types of human failures. Unfortunately poor design of alarm systems has often contributed to errors, mistakes and deliberate violations.

1.4.2. Human reliability assessment.

Assessing human reliability is a complex process beyond the scope of this article. The methods available are covered in [HSE 1999] and [Kirwan 1994] and include estimating the probability of individual types of error. The overall human error probability for the response to an alarm is the combination of all the individual error probabilities.

The danger is expecting too much of the operator and particularly placing undue reliance on the operator for safety. [EEMUA 1999] recommends on page 14 “that in no circumstances should an average probability of failure on demand of less than 0.01 be claimed for any operator action in response to an alarm even if there were multiple alarms and the response was very simple. This puts a limit on the level of reliability that should be claimed for any alarm function.” In other words, on average at least once in a hundred times when the alarm is sounded, the correct response will not happen. In addition, even to achieve this level of human reliability, many good design features are required as specified on page 15 of [EEMUA 1999] and Recommendation 6 of [HSE 1997].

1.4.3. False alarms

Another crucial factor is avoiding false alarms. False alarms are not just problems of fluctuating measurement signals or equipment failures; they are often a feature of the design. Low alarms may come from equipment deliberately shutdown for maintenance but with alarms still functioning.

There are also installations that include as alarms all the numerous events that do not require an operator response and thus should not be alarms, for example:

- signals confirming successful operator action
- emergency shutdown (trip) initiators
- duplicate signals
- plant status changes
- journal events

Previous false alarms inevitably lead to delays in the response to real alarms [CTSA 1997].

1.5. Surveys

The UK Health & Safety Executive funded a research project to survey alarm systems in the power and chemical industries and hence identify and report current best practice. The resulting report [HSE 1998] includes a summary of the 96 responses to an Operator Questionnaire that is also Appendix 12 of [EEMUA 1999]. These responses confirmed the problems already described.

Many other companies not involved in the original survey have since used the same Operator Questionnaire with their own operators.

2. What is industry expected to do?

Over 10,000 copies of “Better alarm handling” [HSE 2000] have been distributed. This recommends some more detailed actions in three simple steps:

Step 1: Find out if you have a problem – for example use the Operator Questionnaire [EEMUA 1999].

Step 2: Decide what to do and take action.

Step 3: Check and manage what you have done.

This deals with the current situation but will not prevent us from repeating the same design mistakes. This requires greater awareness of the guidance for alarm systems.

Examples of more detailed actions included in [EEMUA 1999] are:

- review alarm behaviour following all upset incidents to confirm usability

“Better Alarm Management” by A G Foord & R V Lord

- tune alarm settings on nuisance alarms
- adjust deadbands on alarms which often repeat
- eliminate alarms which have no defined operator response
- ensure “critical and high priority” is allocated to appropriate alarms
- review alarms messages which operators do not understand or know how to respond to

3. Where is the guidance?

[EEMUA 1999] includes detailed guidance, checklists and questionnaires. The guide also includes a section on procurement of alarm systems.

3.1. EEMUA Guide principles

The four key principles in [EEMUA 1999] are: usability; safety; performance monitoring and investment in engineering.

3.1.1. Usability

Alarms should:

- be relevant to the operator’s role at the time;
- indicate clearly what response is required;
- be presented at a rate the operator can handle;
- be easy to understand.

This includes providing operators with succinct “job aids” (that are much briefer and more accessible than the material usually used for training) as reminders of the operator response required for specific alarms.

3.1.2. Safety

[IEC 61508] considers an alarm as “safety related” if:

- it is a claimed part of the facilities for reducing the risk from hazards to people to a tolerable level, and;
- the claimed reduction in risk provided by the alarm system is significant.

The contribution of the alarm system to protecting the safety of people, the environment and the plant equipment should be clearly identified. Any claims made for operator action in response to alarms should be based upon sound human performance data and principles.

3.1.3. Performance monitoring

The performance of the alarm system should be assessed during design, commissioning, operation and maintenance, to ensure that it is usable and effective during all operating conditions. Regular auditing should be continued throughout the life of the system to confirm that good performance is maintained. An example of one of the performance metrics is:

Alarms in 10 minutes after major upset

More than 100
20 to 100
Under 10

Acceptability

Excessive
Hard to cope with
Manageable but

3.1.4. Investment in engineering

Contract strategies should be chosen to ensure that alarm systems should be designed to suitably high standards. The required functionality should be specified and a consistent alarm system philosophy provided to all the suppliers. The initial investment in system design should be sufficient to avoid the operational problems and the safety, environmental and financial risks that often arise and that result in overall higher lifetime costs. The particular problems with “packaged units” that include their own alarms should be tackled.

“Better Alarm Management” by A G Foord & R V Lord

3.2. Training

Hundreds of engineers and operators have already attended training courses based on the [EEMUA 1999] guidance described here. All confirmed that their companies trained their operators how to respond to alarms. Many operated processes or transport systems where overload of alarms (floods) happened occasionally. None of those attending the training thought their companies included how to handle alarm overloads as part of their training of operators. Clearly training operators how to handle alarm floods is an essential requirement when operating systems with hundreds of alarms.

3.3. Checklists

[EEMUA 1999] includes numerous checklists, including: characteristics of a good alarm and good alarm messages; design activities; alarm strategy; human reliability requirements; logical processing of alarms; assessing the capability of alarm systems; performance metrics; techniques for improving alarm systems; elements in a user-centred design; alarm priority break points; types of alarms; procurement specifications; and an alarm suppression hazard study process.

3.4. Range of applicability

The original of research on alarm systems in the power and chemical industries also included discussions with operators of batch processes and members of EEMUA and GAMBICA (a trade association representing control and instrument manufacturers.) The principles in [EEMUA 1999] are relevant to energy, process, transport and utility operations.

3.4.1. Smaller systems

The principles in [EEMUA 1999] are relevant to smaller processes and systems but alarms floods are less likely. All the human factors and the four principles described above still apply.

3.4.2. Batch processes

Batch processes are not specifically mentioned in [EEMUA 1999] but the principles are still relevant to batch processes - see the Case Studies 5.1 and 5.2 below. Discussions with the safety managers of companies operating batch processes have confirmed that there is no need for different guidance.

3.4.3. Transport

That the principles above are equally relevant to transport operations may seem surprising when the original research was on alarm systems in the power and chemical industries. Transport systems do include numerous processes and alarms (for example a London Underground station may have thousands of alarms) so similar problems arise. In addition the [EEMUA 1999] guidance is focused on human factors and people have similar characteristics across many industries. Those attending the EEMUA training course from the transport industry have found it both relevant and helpful.

4. How do I demonstrate compliance?

4.1. Management System

A safety management system that includes the usual review and audit facilities; monitors alarm performance; and includes human factors and operator competence should already comply with [EEMUA 1999]. In practice safety management systems have had weaknesses in one or more areas, for example:

- No clear identification of safety related alarms;
- Too many top priority alarms (should not be more than 20);
- No site alarm policy or philosophy so that alarm priorities and grouping are not consistent even within the same control room;
- No records of assessing operator competence;
- No (or inadequate) corrective action following incidents involving alarm floods;
- No performance specifications for alarm procurement.

“Better Alarm Management” by A G Foord & R V Lord

4.2. Records

A safety management system that includes the usual records facilities should already comply with [EEMUA 1999]. In practice records have had deficiencies in one or more areas, for example:

- No records of assessing operator competence;
- Inadequate records of alarm system performance following plant upsets;
- Inadequate records of process performance following plant upsets;
- Inadequate records of alarm testing.

The lack of adequate data about plant incidents and upsets makes it more difficult to specify requirements for alarm systems and to justify improvements. Many computer control systems store history data for only a few months. Off-line storage of data about past plant upsets is essential.

5. Case Studies

5.1. An old batch process

The separate control loops on an old batch process were recently replaced by a modern computer control system. No alarm system policy or usability criteria were specified and as a result the contractor provided a large number of alarms with the computer control system. A visit from an HSE inspector identified:

- signals confirming successful operator action
- duplicate signals
- plant status changes
- journal events

all designated as alarms. There was also no clear identification of safety related alarms. An additional expensive exercise is now in progress to identify the required alarms and move the others to entries in a log file.

5.2. Another batch process

The alarms on a batch process were separate from the individual control loops, but there was no clear identification of safety related alarms. The safety related alarms were specified in the safety case but they were combined with the other alarms on annunciator panels. The problem was solved simply by putting a small sticker directly onto the face of the each safety related alarm display on the annunciator panels and by on-the-job training of the operators.

5.3. A continuous process

The alarms on a large continuous process unit had resulted from many separate projects and the installation of replacement packaged units. Each project and supplier had used a different alarm policy and philosophy. The operators were trained on each of the packaged units separately but the different priorities of the alarms caused confusion and mistakes in responses. A number of high profile incidents have occurred over the past three years. The subsequent investigations, that also involved the HSE, revealed that the inconsistencies in alarm policies had contributed to the operational errors.

The senior management set up a project to produce a site alarm philosophy and to implement this for all new projects. In addition the existing control rooms are being reviewed to assess the changes needed to ensure compatibility with the new site alarm philosophy. This is a major undertaking and it will be five years before all the existing control rooms have alarms that are consistent with the new alarm philosophy.

5.4. A real life challenge

A recent incident was created when the simple change over of oil filters resulted in a compressor trip. The trip of the compressor resulted in loss of hydrogen circulation and hence process upset. During the hectic activities to bring the situation under control, the plant manager noticed that the panel operator was ignoring the alarms. Additional resource was added to acknowledge, read and advise the panel operator of each alarm whilst the operator handled the controls of the process.

“Better Alarm Management” by A G Foord & R V Lord

There are two areas of concern here in that the operator did not have time to look at all the alarms being annunciated and that it needed another person to sift through what was useful and advise the panel operator accordingly. A good alarm system should do this for the operator automatically.

A recent review of alarm equipment revealed that there were several different ways that had been made available to bring warnings to the attention of the operator. Typically, panel indicator lights, lamp boxes, VDU with window box styles, alarm summary displays and graphic displays. All of this on one plant panel for one operator to understand and to act upon. This may have been possible if there had been some measure of priority attached to each type of display. However, this was not the case since the lamps had pump status as well as safety critical alarms adjacent to each other. The lamp boxes had a proliferation of colours that did not signify the correct priority between safety critical and perturbed operations and the alarm summaries were confused with deviation alerts, status indications maintenance warnings as well as perturbed and safety critical alarms. With no alarm philosophy in place, the freedom for individuals to interpret how to best indicate an alert or alarm resulted in a very poor operator information and guidance tool.

Many recent projects have recognised that process alarms would be required. However, the HAZOP has only indicated that an alarm may be considered later since the DCS could easily be configured at a later date once detailed engineering determined the need. This approach is what has caused the proliferation of alarms that presently exist on many systems. This, along with flexibility in DCS that allow operators the ability to configure their own alarms. It is now a requirement at each HAZOP to consider the alarm category (safety, environment or cost) and then allocate a priority (safety critical, high, low or journal). At this stage of any new project this sifts out the unnecessary alarms but more importantly identifies those of a critical nature thereby allowing a more appropriate method to be designed to bring this to the attention of the operator in a meaningful manner. It is essential at this time that the operator is involved to both ensure the description of the alarm is adequate and also to understand the corrective actions to be taken should the demand occur. This philosophy is now working; only time will tell if it is truly successful.

6. References

- [Bransby 1998] “Explosive lessons”, by Matthew Bransby, Computing & Control Engineering Journal, **9** (2) p.57-60, April 1998, IEE
- [Bransby & Jenkinson 1998] “Alarming performance”, by Matthew Bransby and James Jenkinson, Computing & Control Engineering Journal, **9** (2) p.61-67, April 1998, IEE
- [CTSA 1997] “Inquiry into the fire on the Heavy Goods Vehicle Shuttle 7539 on 18 November 1996”, 1997, Channel Tunnel Safety Authority
- [EEMUA 1999] “Alarm systems – a guide to design, management and procurement”, EEMUA publication No. 191, 1999, EEMUA, ISBN 0 85931 076 0
- [HSE 1997] “The explosion and fires at the Texaco Refinery, Milford Haven, 24 July 1994”, 1997, HSE Books, ISBN 0 7176 1413 1
- [HSE 1998] “The management of alarm systems” by M Bransby and J Jenkinson, HSE contract research report 166/1998, 1998, HSE Books, ISBN 0 7176 1515 4
- [HSE 1999] “Reducing error and influencing behaviour”, HSG 48, 1999, HSE Books, ISBN 0 7176 2452 8
- [HSE 2000] “Better alarm handling”, HSE information sheet, Chemicals Sheet No 6, 2000, HSE CHIS6
- [IEC 61508] “Functional safety of electrical/electronic/programmable electronic safety-related systems”, Parts 1, 3, 4 & 5 in 1998, Parts 2, 6 & 7 in 2000, BSI
- [Kirwan 1994] “A guide to practical human reliability assessment”, by B A Kirwan, 1994, Taylor and Francis, ISBN 0 7484 0111 3