

Alarms Management/ Priority, Floods, Tears or Gain?

Introduction to the "problem"

Harry Smith, Colin Howard and Tony Foord

4-Sight Consulting

Alarm systems are a major tool allowing process operators to identify escalating abnormal situations and take action to recover. Such occurrences can quickly lead to personnel danger, environmental damage and commercial loss. The many shortcomings found in alarm systems can cause incidents where the risk to personnel is increased together with an increase in operation costs. *Figure 1* shows how operators respond to abnormal conditions.

Historically alarms have been viewed as an entity in themselves with little thought given to human factors and how they might help an operator investigate the root cause. Information is now available from the Health and Safety Executive (HSE) guide on *"Reducing error and influencing behaviour"*² and from the various papers presented at the *"People in Control"* conference.³

There are many legacy systems which have experienced minimal maintenance over time and whose documentation is either out-of-date or non-existent, leading to conflicts when changes have to be made. For new projects much of equipment manufacture is now given to third parties, each of who may have their own way of approaching alarm needs. If strong management systems are not in place to ensure a consistent human factors approach then potential exists for increasing risks to people, environment and equipment.

Poor management ownership of alarm systems with no agreed alarms policy inevitably leads to a situation where alarms are incorrectly set, giving large numbers of irrele-

vant alarms which the operator, frustrated, begins to ignore or which obscure more critical alarms.

Rationalisation and de-manning of control rooms⁴ without an awareness of human factors further increases potential risks.

When We Get Things Wrong, We Get Them Very Wrong

The Electrical Equipment Manufacturers and Users Association (EEMUA) guide⁵ and² give many examples illustrating the seriousness of the problem. A few high profile examples where absence of good alarm management was a major factor leading to a disastrous outcome are:

- Three Mile Island, 1979 - Operators failed to recognise that a valve was stuck open and this seriously damaged the core of a nuclear reactor.
- Union Carbide, Bhopal, 1984 - A cloud of toxic gas killed over two and a half thousand people. A further quarter of the city's population was affected.
- Herald of Free Enterprise, 1987 - A roll-on roll-off ferry sank rapidly in shallow water and one hundred and eighty nine passengers and crew died.
- Texaco Refinery, Milford Haven, 1994 - An explosion and resulting fires at an oil refinery⁶ injured twenty-six people and caused £48M of damage plus major production loss.
- 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.

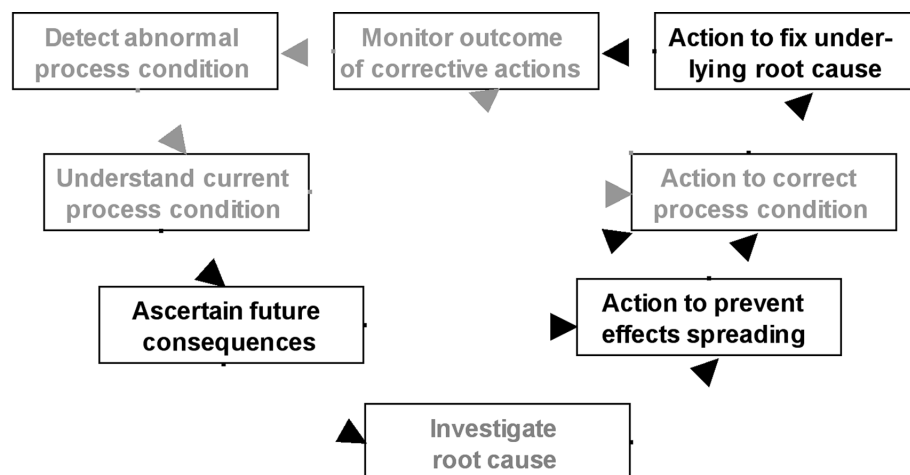


Figure 1: Response to abnormal conditions

Common themes were:

- Poor ergonomics of control panels.
- Distraction of many non-essential alarms.
- Inadequate operator training and communication.
- Poor maintenance management.
- Inadequate safety management.
- Pressure to achieve operational goals overriding safety.
- Absence of effective alarm/reporting systems.
- Absence of any process overview.
- Lack of modification controls.
- False alarms obscuring the real picture.

The potential for "problems" is increasing.

Demands on operators are increasing through:

- The need for process operation close to maximum efficiency;
- Higher costs of process interruptions;
- More complex processes are now possible;
- Lower safety margins giving less opportunity to recover from upsets;
- Environmental regulations mean that venting to atmosphere, direct discharge to waterways or landfill may no longer be acceptable;
- Fewer operators;
- Higher staff turnover resulting in less experienced operators.

Increasing sophistication of control systems and processes means systems being operated in multiple modes by complex computer control with the mental model held by the operator changing significantly over time (Table 1). If human factors, as detailed in² and in the HSE contract research report on "Proposed framework for addressing human factors in IEC 61508"⁸, are not given consideration during design then these starkly different operator roles will ensure a continuation of overload situations and further incidents.

More significantly, it is becoming increasingly difficult for any one operator to understand both the complete process and computer control system.

What Are the Requirements?

The present parlous state of many alarm systems can be improved quite dramatically by initially removing false alarms. Such alarms are not just problems of fluctuating measurement signals or equipment failures; they are often a feature of the design.

There are also installations that include as alarms numerous events not requiring an operator response and thus should instead be routed to a journal log, e.g.:

- Signals confirming successful operator action;
- Emergency shutdown (trip) initiators;
- Duplicate signals;

- Status flags;
- plant status changes.

To achieve strong alarm management cultures and ownership of continuous improvement processes there is much to be gleaned from:

HSE

In the article "Better alarm handling - a practical application of human factors"⁹ Dr. Debbie Lucas, Principal Psychologist, HSE, states "Incidents are still occurring involving alarm systems and there are still significant problems with alarm systems on some major sites. Training, competency and user support are still key areas and users and designers need to be aware of each others' requirements". She goes on to state "We (HSE) expect companies to review their alarm systems from a human factors standpoint and to seek continuous improvement." To assist they have issued an information sheet¹⁰ laying out in three succinct steps the requirements needed to achieve continuous improvement.

IEC/BS 61508

This generic standard defines a whole life cycle approach to the design, commissioning, operation, modifying and decommissioning of installations where safety related functions exist.

IEC 61511¹¹

This standard (part 2 draft) is the interpretation of IEC/BS 61508 specific to the processing industry which specifically focuses on the need to consider human factors for all alarms where credit is being claimed for a risk reduction.

EEMUA 191

This guide, from work by Bransby and Jenkinson¹², provides advice with regard to developing continuing programmes for alarm performance improvement

Alarms Need People - Human Factor Issues

The HSE considers alarm handling to be a continuing major safety issue and has an expectation that businesses review their alarm systems from a human factors perspective and have in place management strategies seeking continuous improvement⁹.

However, ignorance of human factors is widespread and in particular a 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.

Reference² includes a formal definition of human factors based on the task, the individual and the organisation. This definition states: "Human factors refer to environmental,

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

Table 1: Operators process mental model

organisational and job factors, and human and individual characteristics which influence behaviour at work in a way which can affect health and safety". 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.

From the incidents described in references^{5,2} we can identify human failures as:

Errors and mistakes

- Skill-based errors such as taking action not as planned or omitting an action - e.g. not closing the bow doors on a roll-on, roll-off ferry.
- 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 - e.g. not recognising that an alarm is safety-related and needs immediate action.

Deliberate violations

- 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 - e.g. suppressing a repeating or erroneous alarm without following the correct procedure for alarm suppression.
- Situational violations where the rule is difficult to apply, conflicts with other rules, resources are lacking or extreme conditions prevail - e.g. trying to rely solely on control room measurements to avoid going outside in bad weather.
- Exceptional violations where something has already gone wrong which leads operators to justify breaking a rule - e.g. ignoring all alarms during alarm overloads.

Good design of alarm systems will contribute to reducing all these types of human failures.

The danger is expecting too much of the operator and placing undue reliance on the operator for safety. Reference⁵ recommends "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 reliabil-

ity that should be claimed for any alarm function. To achieve this level of human reliability, many good design features are required as specified on page 15 of reference⁵ and recommendation 6 of reference⁶. It is also essential to allow time for the operator to respond (*Figure 2*).

Conflicts Between Various Business Needs

In business there is a need to reduce manning to reduce costs, a need also impacting control rooms. Compounding this situation is the merging of functionality, previously spread over several control rooms, into a single unit. Without consideration of human factors involved under all modes of process operation in respect of total alarm numbers, prioritisation, physical display arrangement available to operator/s and well defined operating procedures for handling critical alarms then the present level of concern will continue.

The difficulty of arriving at any comprehensive cost benefit figure for alarm systems is generally accepted. This is the case whether or not it's a new system, a replacement new for old, or an upgrade to an existing alarm system. As a consequence we have under-investment in both money and design/management effort, leading to increased overall risk.

Important aspects requiring attention at the contractual stage must include:

- Activity allocation - ensuring that such aspects as process design, equipment design, alarm system configuration, human factors, maintenance and plant operation are given to parties with the appropriate skills and experience.
- Activity scheduling - ensuring that the most appropriate timing is carried out to ensure engineering best practice; e.g. install a minimal alarm system initially, building to the final form over an agreed period of time.
- Acceptability testing - there is a clear requirement to initiate a clear test of acceptability of delivered alarm systems. However, proving that an alarm system is functioning correctly will require an extensive operational time period. This requirement can be extremely difficult to define contractually.
- Engineering quality - the engineering requirements must not suffer through any competitive tendering process.

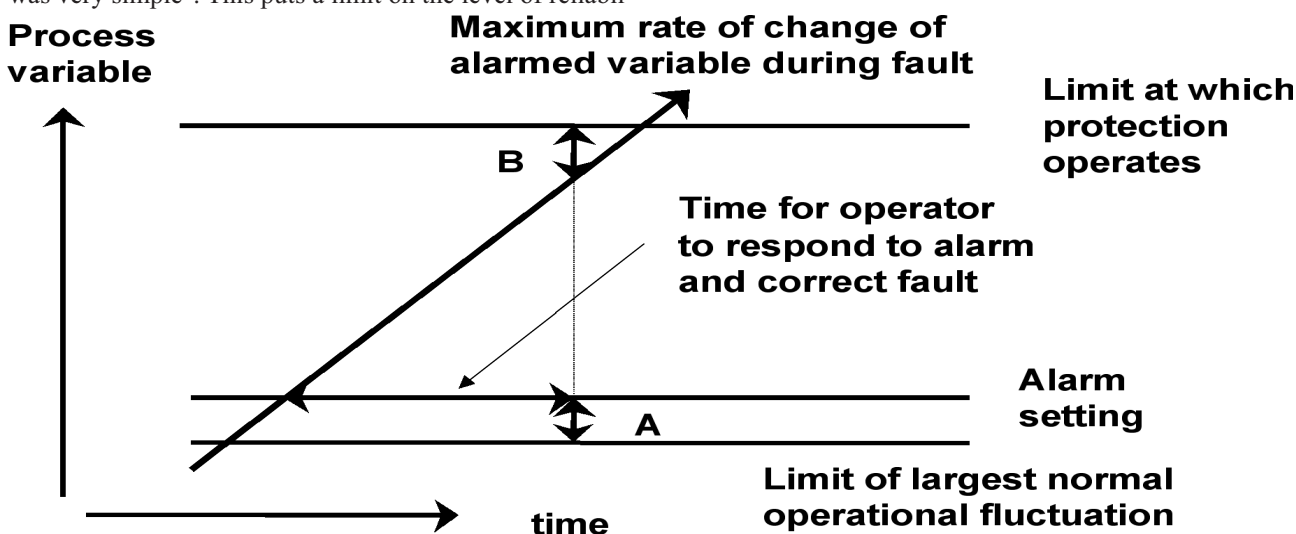


Figure 2: Operator response timing

Demonstration of Compliance

Safety management requirements as defined in reference⁵ need be no different to other accepted management systems which include reviews, audits, performance monitoring, human factors and operator competence. However, 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;
- 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.

A safety management system that includes the usual records' facilities should already comply with reference⁵. In practice, records have had deficiencies in one or more areas, e.g.:

- 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 on plant incidents makes it difficult to specify requirements for alarm systems and to justify improvements. Many computer control systems store history data for only a few months, but it is relatively simple to download to an off-line PC such data for storage and analysis. This is an essential prerequisite to providing the necessary cost benefits argument for system development.

Case Histories

An alarm management review on an existing plant requires consideration of human as well as technical issues. There will have been a significant number of modifications and other changes since original plant design, some of which may not be immediately apparent. Also the original design and the design of subsequent modifications may have introduced weaknesses into the overall alarm management philosophy.

At the start of a review it is important to have a good understanding of current plant operations, be able to identify key changes from the original design philosophy and potential issues impacting alarm management. Typical changes, which may have affected the alarm management philosophy, include:

- Replacement of conventional panel-mounted control systems with computer-based systems. These changes may not have incorporated consistent approaches to alarm management.
- Plant extensions with dedicated control systems not integrated with the original plant.
- Reductions in plant manning, with additional responsibilities placed on individual operators.
- Revised legislation or business operations may have introduced additional requirements on the operations team or on the alarm systems. For example, have business requirements introduced specific time constraints controlling particular plant operations requiring operators to make

rapid and correct responses against fixed deadlines; or has the impact of COMAH or IPPC legislation been reflected in the alarm management philosophy?

- Have training and competence assessments, including realistic emergency scenarios, been updated?
- Changes to the product spectrum requiring different alarm settings and responses by the operations team.
- Society's perceived environmental requirements are increasingly important.

The methods outlined in reference⁵ are key tools to develop and implement an effective approach to alarm management. Any alarm management reviews should not be confined to justification of individual alarms alone, but should look at the context of one alarm with all others related to the particular function. There is also the need to examine the underlying plant design and operating philosophies. Establishing the alarm management philosophy to complement the design and operating requirements is an essential first step requiring time and thought to achieve a robust outcome.

Although hazard studies should have been part of any modification, these may have overlooked key issues, particularly if these were not part of the original design philosophy. Two examples from a recent alarm review highlighted:

- The arrangements for and stability of the site power supply had changed since the original plant was designed. Supply disturbances were resulting in the electric motors on key utilities stopping and the generation of high priority alarms. The plant had never been fitted with delayed under-voltage (DUV) protection for these key drives enabling the systems to automatically recover from short-term supply disturbances. Provision of DUV protection reduces generated alarms, avoiding operators manually restarting service drives at a time when their attention is required elsewhere.
- Replacement of an existing control system with a PLC resulted in the modified system generating many more alarms during power supply disturbances. Supplying the PLC via UPS prevented the shutdowns and generation of unnecessary alarm floods.

Instances of where DCS systems have been extended or upgraded as a consequence of Y2K, but the new extended functionality has not been implemented, have included:

- Enhanced capabilities of the upgraded alarm management system.
- Linking the alarm banner message direct to the point in alarm graphic.
- Terminology to describe or interpret alarms is inconsistent, often being unchanged from the original system.
- Facilities to give different priorities to separate alarms on the same tag (e.g. a high-high level alarm could require a different priority from a low level alarm on the same tag).
- Alarm messages not always conveying useful information due to message constraints in earlier versions of the replaced software.

Where a DCS has been retrofitted to a plant and the conventional panel instruments and annunciators have been retained for part of the plant, the operations interface can become confused. With part of the information on DCS screens and part on the original panel, the operator has to divide his attention between the separate and often disparate process interfaces. A recent example involved six compressors on a common duty, installed over a number of

years, two of which were controlled from a DCS, and four controlled in two separate locations from the original control panel. With the current arrangement, the operator has to monitor three physically separate locations in the control room to obtain the full picture about the operation of the compressors.

Alarm suppression provides significant benefits in removing standing alarms when a plant unit is shut down, provided the meaning of "shut down" is clearly understood. If inventory has been removed as part of the shut-down process and the equipment fully isolated then suppression of all the alarms is likely to be appropriate. However, if the plant is left to allow restart at short notice, with key inventories in place, then there will be a number of alarms that should not be suppressed during plant "shut down".

Accurate information on the alarms installed on the plant is essential for a successful alarm review process. On an existing plant the quality and location of the information can be variable. Effort spent in collating the available information into a core source file is well spent, both for the success of the review and as a basis for a future alarm database.

With the number of alarms installed on any reasonably sized plant the alarm review process requires involvement of operations teams to define the scope and expectations of the review. It is essential that the review process itself is well thought out, in particular with consideration of how to assemble alarms into groups for efficient review, the word models and prompts to be applied and the recording method for the input data and outcome of the review.

Any individual alarm review session should have a clear agenda to ensure focus on the agreed task. Reviewing alarms, and their context with other associated alarms, by unit operations has been found to be the most efficient with a spreadsheet being sufficient for the initial capture of data, risk assessment and subsequent actions.

This approach allows incident scenarios to be tested and the potential for alarm flooding to be explored.

Anecdotal Information from Course Attendees

Over the past three years we have been giving one-day long public and in-house courses on "Alarm System Management". These courses, based around EEMUA publication 191, have attracted considerable interest with participation from a wide range of industry and have provided a number of anecdotal observations.

- Provision of an alarm system is very much an afterthought and its quality is determined by what is left in the project budget rather than safety needs.
- Little performance monitoring of alarm systems exists within industry.
- The aspect of human factors is not generally recognised.
- The industry's understanding of the provisions laid down in IEC/BS 61508 and IEC 61511 is presently very limited.
- Prioritisation is often not carried out, or where it is the ergonomic aspects are poorly implemented.
- Many alarms arise from poorly tuned or unstable processes, cure the process before rationalising the alarms

themselves.

- Much background information on the subject of alarm management is not disseminated effectively.
- There is a need to ensure that operators are involved at the early stages of any new and updating alarm system projects.
- Very few businesses have been identified as having some form of alarm systems management policy and strategy.
- The subject of risk assessment is not fully appreciated or understood.
- Knowing that a typical power station has approximately 5000 alarms, and a nuclear submarine includes a nuclear power station and a large "hotel" plus equipment, it came as a surprise to note a maximum of 35 "Alarms"! This arises from a clear distinction of priorities - between 35 high priority and hundreds, if not thousands, of lower priority 'warnings'.

Conclusions

The EEMUA guide is an effective starting point for any businesses wanting to commence an improvement process for their alarm system management. Though derived from continuous processes, the guide is also applicable to batch processing. There are a number of individual businesses and individual managers who appreciate their predicament; however, they are limited in their rate of improvement by a lack of time and available resources. Our experience from involvement with clients and feedback from the public and in-house courses leads to the conclusion that, whilst work has commenced on improving alarm management, a great deal more needs to be done.

References

1. 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.
2. "Reducing error and influencing behaviour", HSG 48, 1999, HSE Books, ISBN 0 7176 2452 8.
3. "People in Control - Human factors in control room design" edited by Jan Noyes and Matthew Bransby, IEE Control Engineering series 60, ISBN 0 85296 978 3.
4. "Assessing the safety of staffing arrangements for process operations in the chemical and allied industries", Philip Brabazon and Helen Conlin, HSE contract research report 348/2001, HSE Books ISBN 0 7176 2044 1.
5. "Alarm systems - a guide to design, management and procurement", EEMUA publication No. 191, 1999, EEMUA, ISBN 0 85931 076 0.
6. "The explosion and fires at the Texaco Refinery, Milford Haven, 24 July 1994", 1997, HSE Books, ISBN 0 7176 1413 1.
7. "Inquiry into the fire on the Heavy Goods Vehicle Shuttle 7539 on 18 November 1996", 1997, Channel Tunnel Safety Authority
8. "Proposed framework for addressing human factors in IEC 61508" Michael Carey, HSE contract research report 373/2001, HSE Books, ISBN 0 7176 2114 6.
9. "Better alarm handling - a practical application of human factors", Measurement + Control Journal, volume 35 March 2002.
10. "Better alarm handling", HSE information sheet, Chemicals Sheet No 6, 2000, HSE CHIS6.
11. IEC 61511 - "Functional safety - Safety instrumented systems for the process industry sector", parts 1, 2 (Draft) and 3.
12. "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.