

Alarms: prevention is better than cure

David Hatch offers guidance on objective alarm specification to reduce hazards and improve productivity



IN July 1994, a lightning strike at the Texaco Milford Haven refinery started a chain of events that ultimately led to an explosion and several fires. Although the cause of the incident was attributed to failures of management, equipment and control systems during the plant upset, it was also determined that alarms occurred at the rate of one every two to three seconds in the five hours leading up to the accident.

This flood of alarms reduced the operator's effectiveness to respond. As a result, the 'ultimate' alarm, the high-level alarm in the flare drum, apparently went unnoticed for some 25 minutes; then the line ruptured and an explosion followed.

The accident is a stark reminder of the, sometimes unavoidable, human component within control and safety systems and our inability to identify, analyse and act upon key information when under stress or with poor guidance.

As part of its investigation, the Health and Safety Executive (HSE) published 14 lessons to be learned from the accident to improve safety management within the process industry. The lessons include the following guidance relevant to alarm systems:

The use and configuration of alarms should be such that:

- Safety critical alarms are distinguishable from other operational alarms.
- Alarms are limited to the number that an operator can effectively monitor.
- Ultimate plant safety should not rely on operator response to a control system alarm.

These recommendations highlight that where alarms are safety related, ie offering risk reduction, they must be treated as protection systems. The principle of protection layers is summarised in Figure 1.

This illustrates how an operator's response to a critical alarm may be the 'last resort' attempt to bring the process back into control before the safety instrumented system (SIS) or other protection layers have to act. While this is intended to reduce the demand rate of the SIS, if the operator is unable to act correctly this will at best interrupt valuable production or at worst increase the demand on the SIS.

Given these human limitations, our objective must therefore be to increase the operator's ability to perform reliably and repeatedly as and when required.

An obvious starting point is to reduce the total number of alarms to be dealt with so that those that are time- or impact-critical are given preference over less 'important' alarms.

In 1999, the Engineering Equipment and Materials Users Association (EEMUA) produced its Publication 191, *Alarm Systems, a guide to design, management and procurement*, as a set of guidelines for the design, implementation and improvement of alarm systems. EEMUA 191 has become the global 'de facto' alarm reference for designers and operators alike.

measure performance

For new and existing plants or processes, the aim is to implement the minimum number of alarms necessary to ensure the protection of personnel, environment and plant in all operating modes.

The focus should be on alarm prevention rather than cure wherever possible. The HSE study *Out of control: why control systems go wrong and how to prevent failure* found that 44% of studied incidents associated with automated systems were attributed to the failures or shortfalls in the specification.

A system for a typical plant will have hundreds or thousands of alarms

and therefore the reduction must start with evaluating the scale and extent of the challenge before planning how and where to target resources.

EEMUA 191 offers the following simple benchmarks as typical metrics for evaluating the performance of alarm systems.

Average standing alarms	< 10
Post-event alarms	< 10 in 10 minutes
Average alarm rate	< 1 every 10 minutes

To compare actual performance against established targets requires historical data on the alarm system. This information can either be gathered manually or electronically as shown in Figure 2.

Such analysis can identify the source of the alarm, how often it is triggered and how long it takes the operator to respond to it. Appropriate formatting of this information can also identify alarm patterns that show standing, duplicated and recurring alarms.

alarm justification

Alarms are provided to reduce operating risk. Each configured alarm must have a clear purpose and be unambiguous. From EEMUA 191: "Every alarm presented to the operator should be useful and relevant to the operator".

For the justification and evaluation of either new or existing alarms, Figure 3 proposes a simple, structured methodology which is further explained in the following sections.

define the problem

The review starts with the simple definition of an alarm as offered by EEMUA 191: "An alarm will indicate a problem requiring operator attention..."

Quite simply – if there is no problem then an alarm is considered unnecessary. To identify 'true' problems, a disciplined approach is necessary which acknowledges that problems are solely undesirable or unexpected events. A low level in a vessel that is

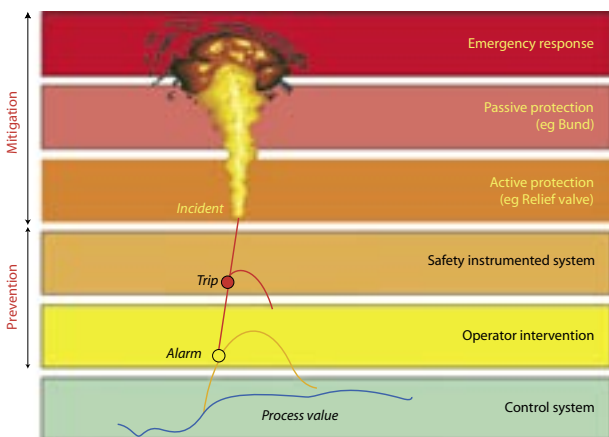


Figure 1: Layers of protection

normally empty or no flow in a pipe without the pump running are expected events and therefore alarms are not appropriate in these cases.

We must therefore evaluate which alarms actually indicate actionable problems. For new or existing plants, HAZOP offers a recognised, objective starting point for problem or hazard identification by systematically assessing process deviations. An alternative for existing facilities is to critically consider each implemented alarm as a problem and justify its retention.

identify the mode

Most plants suffer from standing alarms that are always active regardless of what the process is doing. These can form a substantial background load that increases the demand on the operator during plant upset when he, the process and the equipment can be at maximum stress.

It is important to determine when a problem is not a problem and this is considered in conjunction with the state of the plant or process. This is relevant for multi-purpose batch plants where the operating conditions change according to time and processes and for continuous plants that go through a cycle of offline–startup–online–rundown–offline etc.

By reviewing each plant or process state individually it is possible to remove or reduce standing and other irrelevant alarms.

identify the effect

If no action is taken to address the problem, personnel and production may be threatened. The severity of this hazard and the time until it is expected to occur provides a measure of the criticality and urgency of the alarm. Also the effect (HAZOP consequence) provides the basis for operator guidance so that he knows why he has to carry out certain responses.

The effect of the problem may vary according to the state of the plant and ultimately if the consequence is non-existent or tolerable then an alarm is not necessary for that operating mode.

identify the response

An alarm not only requires operator attention but also some form of corrective action in response to the problem rather than just reflex acknowledgement. Again from EEMUA 191: “The purpose of an alarm system is to direct the operator’s attention towards plant conditions requiring timely assessment or action...” and

“Every alarm should have a defined response.”

Therefore, if no response is required then there should be no alarm. It may be that the control system is required to take some action instead of the operator for reasons of speed, accuracy or remote operation. Typically however, the operator needs to take some manual action, eg opening or closing isolation valves that are outside the control of the control system.

Information to assess likely causes and appropriate actions should be clearly defined and documented. This will ensure that the necessary preventative actions are carried out in time to prevent the identified hazard. Responses should be appropriate to the problem and unambiguous, thereby eliminating the need for the operator to choose a specific action from a possible list of options.

When considering the response of the operator, if there is nothing the operator can do about it – for example, if the event is escalating too quickly for human intervention – then an alarm does not offer any immediate benefit.

Event recording and subsequent analysis may be beneficial to establish the cause of such events but this should not appear as an alarm. If an operator response is not possible then further assessment is required to ensure that adequate layers of protection are in place to prevent or mitigate the hazardous event.

To evaluate the time available for the operator to respond, it is vital to have a full understanding of the dynamics of the process from a heat and mass perspective. That way it is possible to estimate or calculate the escalation time.

identify the indicator

Each configured alarm must be unambiguous and not duplicated by other alarms. Multiple problems should not cause the same alarm, because it becomes difficult to distinguish what the exact problem is. This can mean evaluating more than a single sensor to initiate the alarm.

When reviewing existing alarms consider if there is another alarm which will provide the same information – this avoids alarm echoes as subsequent deviations indicate a problem already identified. Alarm systems which provide ‘first-up’ functionality can discount successive alarms and reduce the demand on the operator. If the operator can be alerted to the problem by another, possibly more reliable, indicator then an alarm is

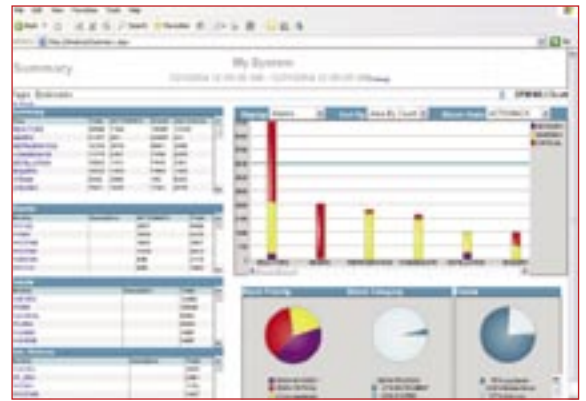


Figure 2: Alarm analysis

not appropriate for the sensor under consideration.

For example, during the Texaco incident the control system indicated that a key control valve was open when in fact it was closed and no flow was indicated. With the latest available digital field technology, equipment failures and process deviations can now be predicted with sufficient warning to prevent abnormal situations.

It is important to consider the process as well as the sensor when assigning alarms. For example, low level

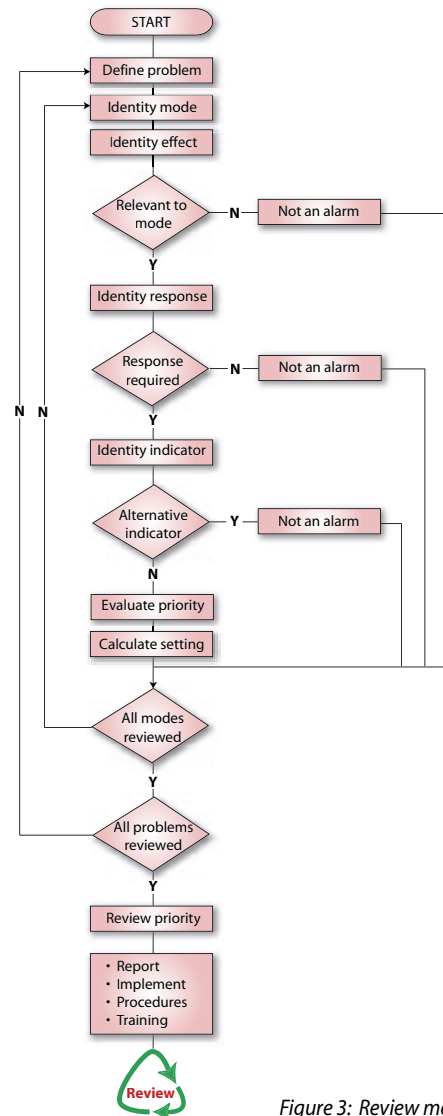


Figure 3: Review methodology

process automation

in a tank may trip a pump resulting in low flow and possibly a low temperature in a downstream heat exchanger.

The loss of flow and temperature are consequences of the loss of level and therefore may be indicated as lower importance to the operator. Equipment or unit-based alarm groups with 'first-up' detection logic can eliminate such duplication, but require knowledge of the process to implement correctly.

evaluate priority

The next stage is to bring the problem to the operator's attention in a way that maximises his effectiveness in dealing with multiple, coincident problems.

The more urgent the problem, the more immediately visible the alarm has to be. If all alarms are presented equally to the operator, they have to make a subjective decision as to what to deal with and when, against a background of the numerous alarms typically generated after a plant upset.

An appropriate approach is to assign a priority to the alarm depending on the consequence and the time to respond. This risk-based method, shown in Figure 4, is similar to one of the qualitative graph methods offered by IEC 61511 to assign safety integrity levels to safety instrumented functions.

For each event (deviation or potential alarm), the impact on personnel safety, environment, asset, production and quality is cumulatively assessed based upon the time to respond, ie problems requiring immediate response are most critical, and summated. The table ranges from major safety impact events that require urgent action and are not appropriate for implementation as an alarm to minor quality impact events that do not require urgent action and all permutations in between.

For example, an event which can result in a minor safety hazard if not addressed within a 'reasonable' period would have a contribution of 128, the impact on the environment may be major if not addressed immediately and would also have a contribution of 128, damage to equipment is not considered possible and therefore the contribution is 0, major production losses will occur in the near future and therefore the contribution is 4 and product quality will be severely affected in the next few minutes so the contribution is 2. This event would therefore require an alarm with a relative priority of $128+128+0+4+2 = 262$.

The risk table must be calibrated to qualify the specific process and plant

circumstances because what may be considered major for one facility or company may be considered minor for another. The time to respond must also be quantified, typically 'urgent' is less than three minutes. The table can be extended to consider other categories or classifications and is shown in its simplest form for clarity.

For all new deviations and existing alarms this structured, objective approach takes account of the total impact of the event and thus can separate the events into a spectrum of visibility.

calculate setting

For analogue measurements, the setting of the alarm value has to maximise the time available to respond and also minimise spurious initiation within normal disturbances of the process.

Often alarms are set at typical values relative to the measured range, eg high at 90%, low at 10%, without further consideration of the time available to respond and process fluctuations. An appropriate knowledge of the process is required to set alarm points which give the operator the right balance of time to respond between too late (tripped) and too early (spurious).

review priority

The review process continues until all states have been evaluated for each problem, and all problems have been examined. At this point, a list of necessary alarms is available which have been objectively graded for priority. In order to be able to distinguish the urgent alarms from the less important alarms some form of relative classification is necessary.

While three or four alarm priorities are typically used, this number may vary based on plant operating philosophy. What is important is that the operator can differentiate effectively between the priorities and the relative balance of alarms assigned to each priority. EEMUA 191 suggests that < 1% of alarms be critical, 5% high priority, 15% medium and the remaining 80% low priority.

With these guidelines in mind, and since all alarms have a relative priority, one can use these ratios to define the alarm priority. Again, these are only guidelines and must be adopted sensibly and consistently according to process and project conditions.

It is worth noting that the control system for the Texaco refinery was configured with some 87% high priority and 13% low priority alarms so it was difficult for the operator to 'see the wood for the trees'.

		Normal	Urgent
Safety	Major	256	N/A
	Minor	128	256
Environment	Major	64	128
	Minor	32	64
Asset	Major	16	32
	Minor	8	16
Production	Major	4	8
	Minor	2	4
Quality	Major	1	2
	Minor	0	1

Figure 4: Priority risk table

execution

The methodology is designed to complement existing hazard and risk assessments and should ideally be done in conjunction with them for maximum effectiveness and efficiency. A multi-disciplined team, similar to HAZOP, provides the breadth and depth of study to deliver a comprehensive report. This should detail the findings of the study with recommendations on implementation, operating procedures and training plans.

An ongoing process of review and improvement ensures that alarms are continually managed to optimise operator reliability and maintain the necessary level of protection. This should include regular audits of system and operator performance based on statistical analysis of alarm data.

conclusion

Properly specified, designed, installed and maintained alarm systems can ensure personnel safety and process security.

Alarms are a human-based function and are therefore subject to error. To enable an operator to respond effectively, they must be provided with sufficient time and information to make decisions under pressure.

Minimising the number of alarms reduces the operator load but must be done objectively and holistically to ensure that key alarms are not omitted or masked by less important or irrelevant information.

Further general guidance on alarm handling is available in the HSE information sheet *Chemicals information sheet 6 – better alarm handling* and the HSE Contract research report 166 – *The management of alarm systems*. **tce**

David Hatch (davidhatch@emersonprocess.com) is an SIS lead for Emerson Process Management; he is a Fellow of the Institution of Chemical Engineers and an IChemE-registered safety professional