HOW TO ACHIEVE 90% OF THE GAIN WITHOUT TOO MUCH PAIN

C R Timms,
Director, C&C Technical Support Services Limited

INTRODUCTION

Anyone who has been involved in the application of IEC 61508 (1) and the Safety Integrity Level (SIL) determination for Safety Instrumented Functions (SIF) will appreciate the amount of effort and tenacity that is required to undertake the task. However, the SIL determination of Safety Instrumented Functions, or trip functions as they are often called, is only the tip of an iceberg when we come to consider what is involved in reviewing or configuring a typical alarm system.

A medium sized process facility may have a few hundred or so primary SIF protective functions that need to be assessed and assigned an appropriate SIL, but the number of alarms configured into a process control system (PCS) that need to be assessed and prioritised can often run into the thousands. The requirements for alarms usually involve different disciplines such as instruments, process, maintenance and the operators themselves. The latter often have the misconception that their life will be easier if they have alarms on everything. Thus the demand for more alarms, along with the ease of configuration afforded by PCS's, regularly leads to a proliferation of alarms. In other words, alarm configuration can all too easily get out of hand.

There is synergy between SIF protective functions and alarms because they both make a contribution to reducing the risk of having unwanted events, and both need an assigned criticality. It is also important to be able to determine when an alarm should be upgraded to the provision of automatic protection, and conversely, when a trip can be downgraded to alarm status.

A SIF is engineered to provide protection against some kind of failure, and has a concise and automatic role to play when a process moves out of its normal operating envelope. Using the best practice IEC 61508 methods, the criticality of the SIF can be assessed as a Safety Integrity Level (SIL) and this is related to the consequences that would occur if the SIF were to fail on demand. These consequences can be any combination of safety, financial and environmental impact.

An alarm function works through the human interface – 'A Methodology for Alarm Classification and Prioritisation' – Timms (2) - to provide an early warning that the process has moved away from the normal operating envelope to:

- Alert the operator to disturbed plant conditions,
- Provide indication of further developments that may need attention,
- Trigger a trained operator response.

Since alarms are part of the overall scheme of risk reduction Figure 1, the criticality of the alarm should also be assessed in order to set an appropriate priority. It makes sense to assess the criticality of an alarm in a similar way to a SIF but based on the consequences that would follow if the alarm fails or is missed by the operator.

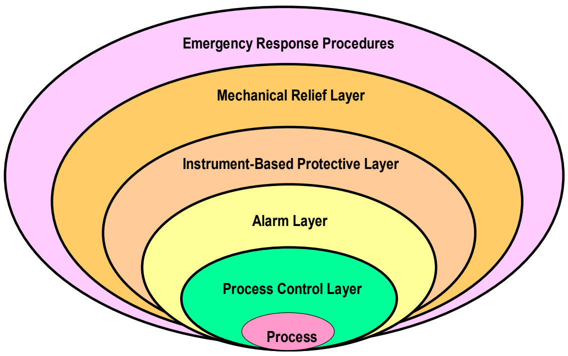


Figure 1: Risk Reduction Layers

However, the contribution that an alarm makes to risk reduction can become clouded if the operator cannot identify the important alerts against a background of alarm problems. The three main problem areas that can potentially compromise safety, production and the environment are:

- Nuisance alarms.
- Standing alarms.
- Alarm avalanches or floods.

Nuisance alarms and standing alarms are usually caused by instrument faults, out-of-service equipment or inappropriate limit and/or dead-band settings. They can be relatively easily identified and rectified by maintenance or adjusting the configuration parameters. However, alarm avalanches or floods are usually the result of consequential or secondary events following a primary event, and the more alarms that are configured; the more there are to appear before an operator in a plant upset condition. The problem for the operator is how to distinguish between the primary initiating event and the secondary consequence events.

Therefore need to rationalise the alarm system in order to alert the operator to alarms in order of importance, so as to give him/her the best chance to take corrective action. Inability to take corrective action can have significant safety, economic and environmental consequences. We must also eradicate those alarms that serve no purpose as this will significantly reduce the alarm overload. This can be achieved by a well defined methodology, and the effort can be significantly reduced by engaging specialist software tools as discussed later.

THE HSE POSITION

The HSE often use the Texaco Refinery explosion in 1994 as the prime example of how the poor application alarms and human factors can result in serious incidents. This paper is not going to regenerate the HSE findings, but their position on alarm handling has been made very clear. They have produced an HSE information sheet ‘Better alarm handling’ (3) to provide some basic guidance, and the Hazardous Installations Directorate (HID) have outlined their strategy with respect to inspection and enforcement, and their expectations with respect to users and designers, in a recent article ‘Better alarm handling – a practical application of human factors’ (4) published in the Measurement and Control magazine (March 2002).

In both publications the HSE guidance provides a simple 3-stage approach:

- Find out if you have a problem
- Decide what to do and take action
- Manage and check what has been done

The HSE also reference the EEMUA guide (5) as ‘the nearest thing to a standard currently available’.

UNDERTAKING AN ALARM REVIEW

The initial reaction when faced with alarm problems can often be to look for ways of using technology to suppress unwanted alarms. PCS vendors are eager to demonstrate how sophisticated their technology can be and commit their customers to using these techniques. There may be possible scenarios where suppression of alarms is simple (e.g. main and standby equipment with auto changeover) but as a rule, the more complex the plant then the more complex the suppression scenarios, leading to very time consuming and complicated solutions. It is also all too easy to loose the focus in the complexity, resulting in an outcome that could be flawed and hence compromising alarm integrity.

An alarm flood reduction will almost certainly require a rationalisation process to challenge each alarm and reduce the number of configured alarms. In essence, an alarm review following the methodology outlined below in conjunction with software tools to aid the process will achieve the most significant benefits. Channelling efforts into this type of activity should be the first priority.

Software Tools will help

The quantity of data to be manipulated, sorted and rationalised will often be considerable, and can amount to thousands of alarms on a modest size process facility. It makes little sense to undertake an alarm review as a paper exercise since dealing with large numbers of alarms will simply overwhelm those involved in the process, and the final paper report will be hard to manage as it will only represent a snapshot in time   It can be tempting to use spreadsheets to manipulate the data, but they are not the most appropriate solution since they do not have the integrity or sorting power afforded by database based approaches.

In this context, it is sensible to invest in the aid of a good software application tool as the first step to managing and maintaining your alarm configuration, and the integrity of a 'master' alarm database. Experience shows that the best tools are database based with a good user interface will facilitate the manipulation and sorting of the large quantities of data involved in an alarm review and save considerable time and effort in the execution of the process. Figure 2 shows an example of a typical alarm data form which could be manually populated, but the advantage of a database structure, is that it can be pre populated from bulk data exchange vehicles such as simple spreadsheets. Each alarm will then have an entry in the master database with the typical of parameters shown in Figure 2. These parameters are the 'keys' for the sorting and grouping of alarms to aid the all important prioritisation and rationalisation process that then follows.

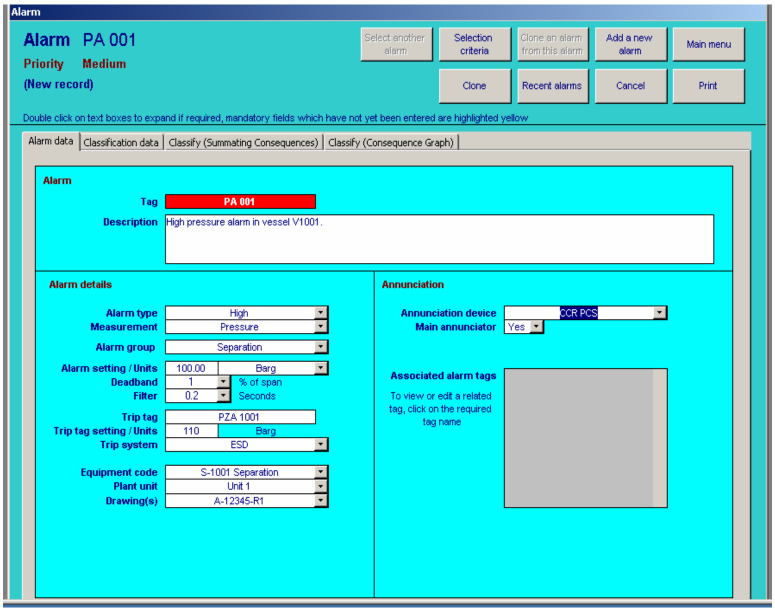


Figure 2: Typical alarm data form

Some tools can be PCS system specific, but the best choice will be an open system tool with the capability of importing an alarm configuration from any PCS, via a suitable data exchange or conversion.

An appropriate tool should then be capable of performing the following:

- Importing the PCS alarm configuration
- Sorting on various alarm parameters such as type, group, measurement
- Selection by parameter or type
- Cloning new alarms from existing alarm template
- Cloning a selection from an existing template
- Performing alarm prioritisation
- Producing alarm metrics
- Maintaining the master database configuration

- Exporting alarm configuration to the PCS.
- Producing reports and statistics

METHODOLOGY

The methodology for undertaking an alarm review detailed in this paper embraces the EEMUA (5) and HSE (3) guidance, but it has been enhanced to offer a very practical and pragmatic step-by-step approach to achieving a high degree of success on established brown field facilities or proposed green field developments.

It will also describe how software based tools can significantly improve the process.

The team

It is essential to set up an optimal alarm review team to provide productivity and quality of output. A small team is recommended for alarm reviews:

- a process engineer, preferably with operational experience, to interpret process design information and to ensure that the design intent is not compromised;
- a control room operator, preferably from the facility under review, to provide information on operator requirements and likely plant dynamics and to ensure that the alarms provided meet the needs of operational personnel;
- an automation and control engineer, preferably with experience of the relevant type of PCS, to advise on aspects of implementation and to ensure that the proposed alarm changes are correctly described for implementation personnel.

For large review studies, it may be desirable to assign a team leader or facilitator to ensure that the correct balance is struck between effort and results. Such a person must have a good understanding of the alarm review objectives and methodology, and should preferably have previous experience of alarm reviews.

Planning

It is anticipated that there will be seven main review phases:

1. Management Plan
2. Preparation of documentation and data sourcing
3. A review of alarm system performance
4. Categorising and grouping of alarms
5. Prioritisation and rationalisation
6. Assessing results and findings
7. Other considerations e.g. alarm suppression
8. Implementation of the changes

A planning schedule should be set up for each phase.

Management Plan

There has to be management buy in before an alarm review can proceed as significant time and and resource have to be committed. Remember that alarms that are missed or not acted on by the operator can lead to trips so develop a rationale for the alarm review which defines the problem with an analysis of the following:

- Detail s of the number and frequency of trips
- Estimates of the cost of loss production
- Details of unsafe consequences (e.g. near misses, in juries)
- Details of any environmental impact (e.g. increased flaring)

Provide estimates of the cost and duration of the review and predicted payback from improved performance.

Preparation of documents and data sourcing

The following documents must be available at the start of the review:

- alarm schedule in suitable electronic format;
- P&I diagrams;
- shutdown Cause and Effect drawings;
- details of fire & gas system;
- details of any controlled sequences;

- configuration details for any complex points, such as digital composites;
- a list of standing alarms during typical steady operation;
- alarm journal print-outs following typical upsets.

The following documents would also be useful:

- a definition of the PCS network configuration;
- a definition of any application programs handling data within the PCS.

To minimise delays, all preparatory work should be done prior to the team convening so that no valuable time is lost during the review process.

A review of alarm system performance

Using alarm journal printouts or output from other dedicated logging facilities, review the existing alarm system performance in order to identify alarm frequency, nuisance alarm sources and standing alarms. Whatever type logging facility is used it must be fast enough to provide true sequence of events recording (SER). Logging facilities on PCS systems can fail to have sufficient speed and buffer capacity to capture the real time snapshot of events resulting in SER overload and indeterminate time stamping.

Each nuisance alarm should be subjected to a detailed review to determine if it caused by a fault or inadequacy in a measurement instrument or the actual alarm configuration. If it is the latter then the alarm trigger point and dead-band should be checked to see whether adjustment of these parameters would eliminate the problem.

If possible, obtain logs of alarm performance under a variety of process upset conditions as this will provide an indication of the number of alarms generated and the frequency at which they are generated. Compare these figures with Appendix 11 of the EEMUA guidelines (5) which sets out guidance on performance metrics.

The majority of standing alarms materialise from spared equipment which is not running spared or that operate intermittently. List any associated alarms that will be active when the equipment is shut down, or put on stand-by, as a source of generating standing alarms when the plant is operating normally. These will be prioritised as outlined in the next section.

Categorising and grouping of alarms

The alarm schedule must be broken down into categories to match the major functional groups of alarms that will be considered during the review, as this will reduce the time involved in the next phase which will be actual prioritisation and rationalisation process.

This categorisation exercise is where the use of software tools can provide a powerful aid to the facilitation and preparation of a comprehensive the alarm schedule. Providing the selected tool has a comprehensive data structure, as described earlier, it is a simple matter to sort alarms on a wide range a of parameters such as tags, alarm groups, alarm types (e.g. High, high high, low, low low, open, closed, not open, not closed), measurement types, annunciation device, alarm priority, plant unit, equipment codes etc. This grouping process dramatically reduces the effort involved in the next stage which is prioritisation.

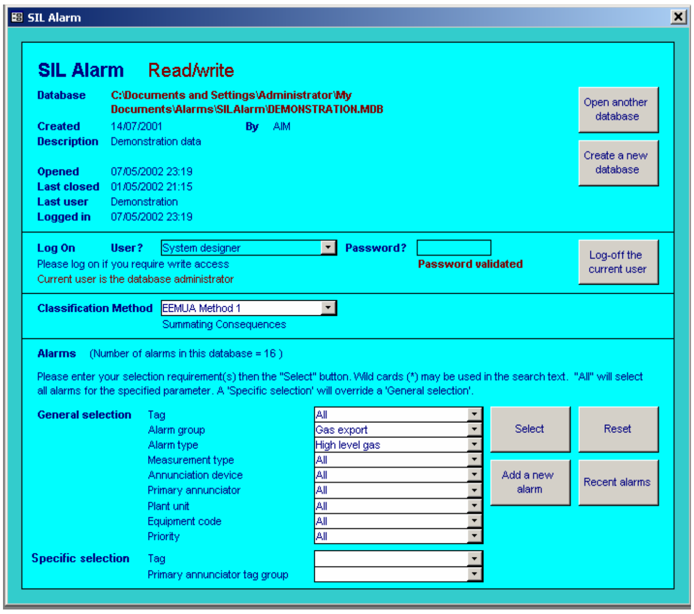


Figure 3: Example of an alarm categorisation form

Each grouping is prioritised as a single entity as detailed in the next section.

It is likely that many of the alarms to be considered during an alarm review process will not be covered, by the functional groups as discussed above. These will be readily revealed from a database and they will have to be reviewed individually.

Determine primary annunciation

It is also important to determine the primary point of annunciation for each alarm e.g. the PCS, Fire and Gas panel, individual graphic tile etc., as many alarms are often repeated and this is a common source of alarm overload. This type of problem is likely to occur when alarms are brought into the PCS from an external system such as Fire and Gas or Safety Instrumented System logic.

The prioritisation and rationalisation process

The EEMUA guidelines (5) Appendix 5 details two methods for prioritising alarms as 'Taking The Maximum Consequence' and 'Summating Consequences'. Both methods are available in the Asset Integrity Management SILAlarm software package and are explained below.

1. Taking the maximum consequence: IEC 61508 SIL determination is a risk-based assessment of the consequences that would arise from a SIF failing to operate correctly, where risk is a combination of probability of occurrence and the degree of harm arising from the consequence. This methodology uses a similar approach for setting alarm priorities but it is focused entirely on consequences because the regularity of the alarm occurrence has no bearing on its priority i.e. an "Emergency" alarm will indicate an emergency condition whether it occurs once a year or once in ten years. The priority of the alarm should be set purely on the severity of the consequences of an unwanted event occurring. Therefore, if operators are presented with highest priority alarms, they will also be addressing those with the worst potential consequences.

The EEMUA (5) 'Taking maximum consequence' method has been enhanced to strengthen its practical application, and provide a consistent and transparent interchange between alarms and automatic SIF protection criticality. It also highlights those instances where an alarm does not provide sufficient risk reduction, and automatic protection is required.

The prioritisation process assesses the consequences resulting from of an alarm failing, for some technical reason, or is missed by the operator. This assessment considers the following factors:

- the consequences of the resulting event in terms of personnel safety, financial loss and environmental impact;
- in the case of personnel safety, the probability of personnel being present in the danger zone at the time.

As an example, if a plant trip were to occur after an alarm was missed, then this could result in economic consequences from lost production. The priority is then based on the severity of the consequences.

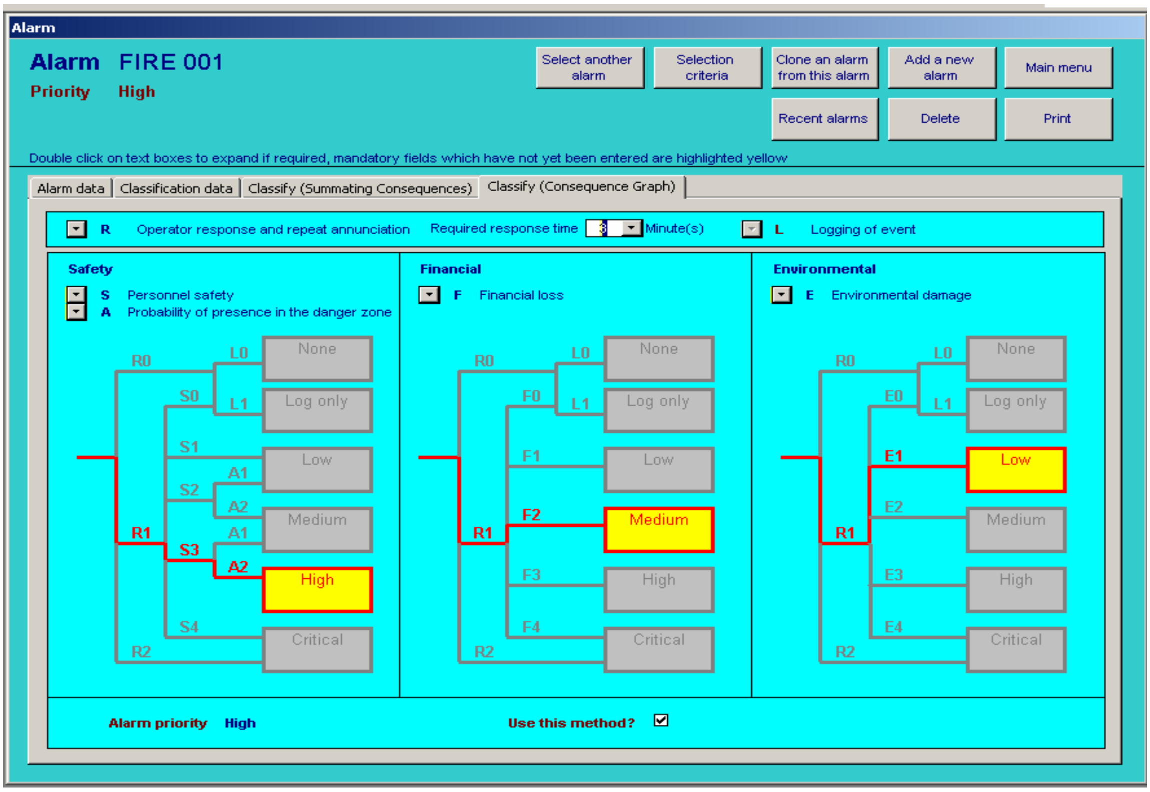
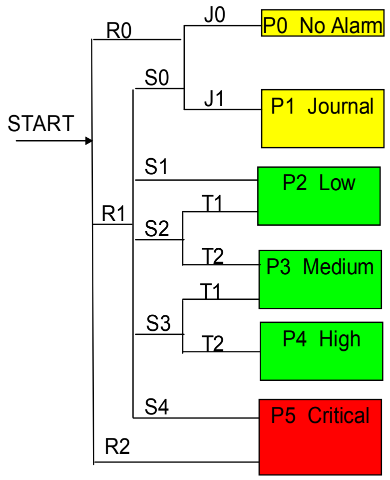


Figure 4: Consequence graphs

Figure 4 shows an example of consequence graphs based on the EEMUA (5) Personnel Safety, Financial Loss and Environmental Damage graphs. They have been slightly adapted to help with practical application.

The selections that are made for operator response (R), safety consequences in terms of the degree of severity (S), journal requirements (J) and presence in the danger zone (T) factors that are selected to establish the safety priority are described in Table 1.

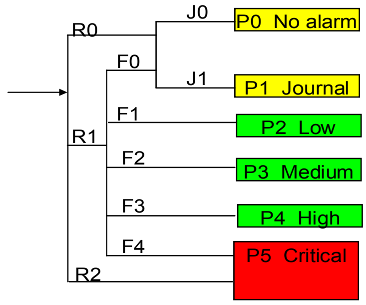


Safety consequences graph

Factor	Qualitative definition
R0	The operator is unable to respond in a timely and effective manner
R1	The operator is able to respond in a timely and effective manner
R2	The operator is unable to respond but consider automatic protection
J0	No requirement to journal, and no activated graphic status
J1	Needs to journal, and/or activates grahpic status change
S0	No possibility of injury
S1	Negligible risk that failure to respond to alarm will result in injury
S2	Remote possibility of injury
S3	Potentially dangerous situation, some possibility of risk of injury
S4	Dangerous situation with a real potential for injury/death
T1	Rare to more often exposure in the hazardous zone
T2	Frequent to permanent exposure in the hazardous zone

Table 1: Personnel safety consequence factors

The consequence factors for making the financial Loss priority assessment are described in Table 2.



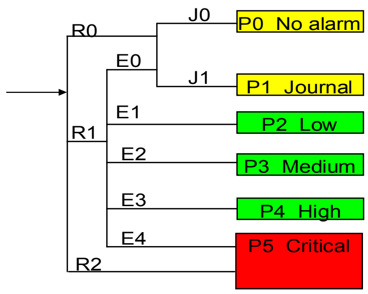
Financial consequences graph

Factor	Financial Qualitative definition
F0	No plant damage or loss of production
F1	No immediate likelihood of plant damage but the possibility of this has increased. Minor loss in productivity or efficiency
F2	Some chance of minor plant damage. Significant reduction in plant output, for example, 10% reduction for 1 hour.
F3	High chance of minor plant damage, low chance of serious plant damage. Significant loss of production, loss of an hour of total plant
F4	High chance of serious plant damage. Serious and prolonged output loss, for example, loss of one day of complete plant output

Table 2: Financial consequence factors

Financial losses are the combination of consequences on production loss and equipment damage that could result if an alarm fails or is missed by an operator. They can be described in qualitative degrees of severity or calibrated in cash terms.

The consequence factors for making the financial Loss priority assessment are described in Table 3.



Factor	Environmental Qualitative Definition
E0	No environmental impact
E1	Negligible risk that failure to respond to alarm results in any breach of environmental limits
E2	Remote possibility of breach of environmental limits
E3	Situation with some possibility of breach of environmental limits
E4	Situation with a real potential for serious breach of environmental limits.

Table 3: Environmental consequence factors

Environmental consequences are the degree of damage that could be caused to the environment if an alarm fails or is missed by an operator. They can also be described in

qualitative degrees of severity or calibrated in limits set by local environmental regulations.
The final alarm priority selected is the highest priority from the Safety, Financial and Environmental

Where priority $P = \max(P_S, P_F, P_E)$

The alarm priority types and their respective configuration attributes are described in Table 4. They indicate a range of alarm requirements from no alarm required ‘P0’, through to the most stringent priority ‘P5’.

The alarm priority annunciation and display attributes that are provided are offered only as guidance for implementation, and individual interpretation is possible providing the design ensures that there is appropriate segregation and presentation at the human machine interface.

Alarm Priority	Alarm Annunciation and Display Attributes
P0	No alarm is required.
P1	No alarm annunciation, but the change of state is recorded in alarm and event journals.
P2	A “Low Priority” alarm with an audible tone is generated and the change of state is recorded in alarm and event journals. The alarm is displayed on the Alarm Summary displays if it is within a PCS.
P3	A “Medium Priority” alarm with an audible tone is generated (a different tone to P2 “Low Priority” alarms) and the change of state is recorded in alarm and event journals. The alarm is displayed on the Alarm Summary displays, if it is within a PCS, and the Alarm Annunciator display if configured.
P4	A “High Priority” alarm with an audible tone is generated (a different tone to P2 and P3 priority alarms) and the change of state is recorded in alarm and event journals. The alarm is displayed on the Alarm Summary displays, if it is within a PCS, and the Alarm Annunciator display if configured.
P5	A “Critical” alarm with an audible tone is generated (a different tone to that used for P2, P3 and P4 alarms) and the change of state is recorded in alarm and event journals. **Alarms of P5 priority should not be configured within a PCS environment as the equivalent SIL 1 or greater**. The alarm facility used should have the appropriate PFD. Full consideration should be made to provide automatic protection.

Table 4: Alarm priorities and attributes

2. Summating Consequences: This EEMUA (5) method is a more complex approach that requires far more detailed consideration. The consequences of an alarm failure, with respect to safety (CS), environmental (CE) and financial (CF) consequences, all have to be converted into common units. In order to achieve this common unit of conversion the safety and environmental consequences have to be expressed mathematically terms of risk.

Figure 5 shows how the required conversions and algorithms can be implemented in software to simplify the prioritisation process.

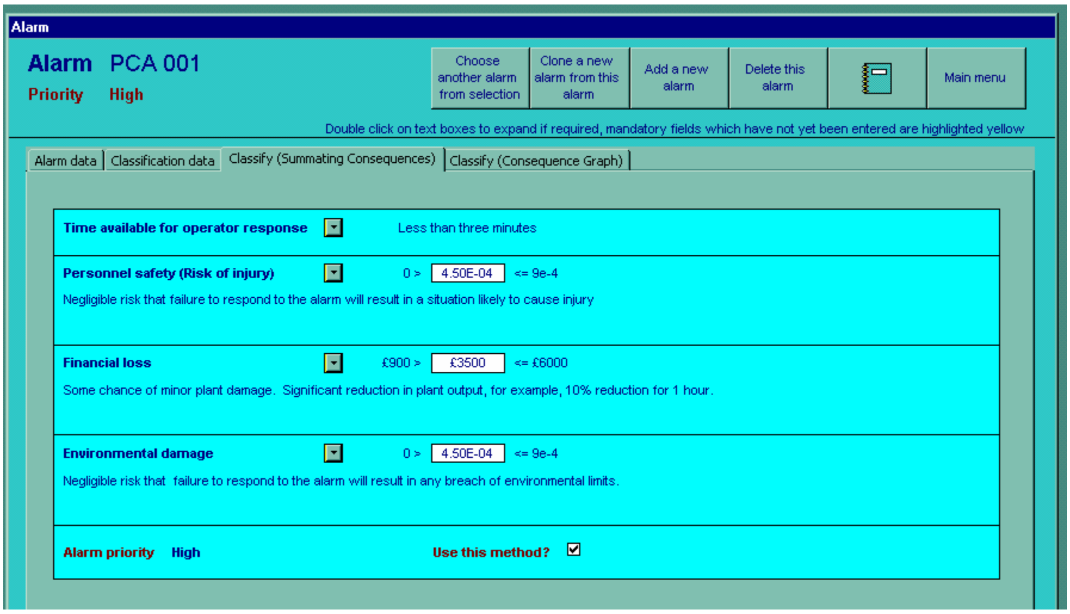


Figure 5: Summating the consequences method

An example of the conversion factors could be as follows:
CS = 10E6 x (safety consequences in terms of risk of injury)

CE = 10E6 x (environmental consequence in terms of risk of injury)

CF = 1 x (financial consequences in pounds)

These are then summed:

C1 = CS+CE+CF

An assessment is then made as to whether the alarm is ‘time critical’ based on whether there the operator is required to respond within say 3 minutes. This is used to increase the weighting on time critical alarms:

IF (alarm is time critical) THEN

C2 := 38C1

ELSE

C2 := C1

The final priority distribution determines the priority:

Weighted total consequence, C2	**Priority**
C2 <900	Low
900 < C2 < 6,000	Medium
6,000 < C2 < 150,000	High
C2 > 150,000	Critical

Dealing with Standing alarms

From the P&IDs, identify items of equipment that are started and/or stopped automatically. Review whether the tags that perform these automatic functions will generate nuisance alarms. If this is the case, identify a way of avoiding this so that normal operation does not generate any alarms but deviation from expected operation is detected and alarmed.

Review each alarm to establish whether it can be reduced to “Journal” priority. If this is not possible, then set the priority in accordance with the consequence of failure method. If any alarms remain with “Emergency” or “High” priority, review whether it is acceptable for these alarms either to be left as standing alarms or inhibited by the operator under procedural control. If neither is acceptable, then identify another PCS tag or combination of tags that indicates that the piece of equipment is out of commission and use this as a criterion for masking the alarm. Confirm that this will not mask the alarm under any other undesirable circumstances. Document the proposed changes and any associated logic.

Assessing the results and implementing the findings

It is important to review the results and finding of an alarm review to check that the right balance has been made between alarm numbers and the respective distribution of priorities. Sort the alarms into their priority groups and compare the results with the distribution in existence prior to the review.   Figure 6 shows a distribution of alarm priorities generated from the results of a typical alarm review.

If the alarm priority distribution indicates an imbalance of higher priority alarms this can be normalised by selecting groups of alarms and applying a revised priority assessment to a whole group.

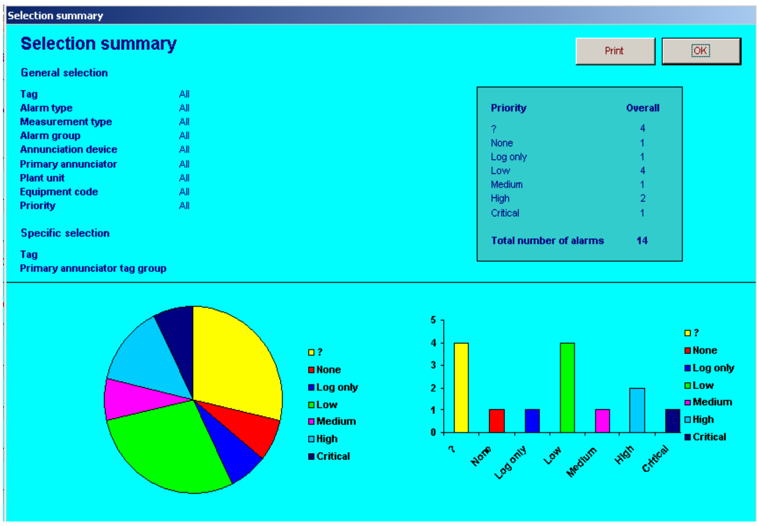


Figure 6: Alarm priority distribution

The EEMUA (5) guidance for new alarm system design advises a target distribution as shown in Table 5.

Priority band	**Alarms configured during design**
Critical	About 20 altogether
High	5% of total
Medium	15% of total
Low	80% of total

Table 5: Priority distribution for system configuration – EMMUA

All alarms with a P0 priority can be removed from the alarm configuration. All ‘P1’ alarms can have their operator annunciation capability removed but they retain their status change as a record in the alarm journal.

Experience shows that the majority of alarms configured into a typical PCS will fall into the ‘P0’ (no alarm required) and ‘P1’ (journal only) following a prioritisation review. Thus the major part of the simplification
and rationalisation of the alarm configuration is going to be achieved by attending to these two alarm types.

Alarms with priorities ‘P2–P4’ should be implemented with the configuration attributes as described in Table 3. Alarms with the ‘Critical’ priority ‘P5‘ require careful treatment since they indicate a SIL requirement of SIL1 or greater. The provision of automatic protection should be considered to replace the dependence on the alarm and successful operator action for each P5 alarm. If automatic protection is not possible, then the alarm must be engineered to achieve the appropriate probability of failure on demand (PFD) in line with IEC 61508 requirements. The EEMUA (5) accepted PFD_{avg} for an alarm with operator intervention is < 0.01 which is only equivalent to SIL 1.

Other Considerations

This paper does not intend to cover the options of static and dynamic alarm suppression in detail, because it is a complex subject area that requires careful implementation. It is anticipated that the requirement to consider these options will be minimised by a thorough review.

Static Alarm suppression

If operators still find difficulty with the quantity of standing alarms present, following the alarm rationalisation, then consideration can be given to the implementation of static alarm suppression. This will minimise the number of standing alarms that are generated when a process unit or large piece of equipment is shut down. In order to suppress the selected alarms, a defined set of process permissives have to be satisfied in conjunction with a with an ‘enable’ static suppression status condition.

Dynamic Alarm Suppression

In addition, if the number of alarms generated following a trip is still unacceptable following the alarm rationalisation, then dynamic suppression can be considered so that the first up alarm in a pre defined group audibly alerts the operator, registers in the alarm list and is printed. All other subsequent alarms in the group do not activate any audible alert; they do not register in the alarm list and are not printed. Dynamic suppression on an alarm group should automatically de-activate after a defined period of time following the first up alarm, so that any new alarm that then follows alerts the operator and re-starts the suppression period.

CONCLUSION

Alarm management requires considerable effort, commitment and tenacity.

However, by focussing effort on an alarm review and rationalisation process, then experience shows that this will return a significant, and perhaps even a dramatic, improvement in alarm performance to achieve better than 90% of the available benefits. There will possibly be some alarms that need further analysis but having filtered them out by the review process they should only represent the remaining 10% of effort.

The review and rationalisation methodology has been applied on facilities with >15,000 configured alarms where individual operators were required to accept alarms every 15 seconds under steady production conditions. Typically, over 50% of the configured alarms have been removed, and by also attending to the nuisance alarms the alarm rates have been reduced to 15-20 minute intervals. Perhaps most importantly the spurious shutdowns resulting from missed alarms have seen improvements from weekly plant trips to no trips for over six months. This results in a very, very significant payback.

Making full use of software tools will substantially reduce the effort involved in an alarm review, whilst the electronic version of an alarm database will provide data integrity along with ease of maintenance and change control over the full life cycle.

REFERENCES

1. IEC 61508 - Functional safety of electrical/electronic/programmable electronic safety-related systems.

2. 'A Methodology for Alarm Classification and Prioritisation' – C Timms – IEE People in Control Conference 1999.

3. 'Better alarm handling' – HSE information sheet – Chemicals Sheet No. 6

4. 'Better alarm handling – a practical application of human factors' – John Wilkinson and Dr Debbie Lucas - Measurement and Control Volume 35.

5. 'Alarm systems – A guide to design management and procurement' – EEMUA publication No. 191.

Biography:

Clive Timms

Clive has over 38 years experience in the petrochemical industry with offshore and onshore plants experience. He recently retired from Shell UK Exploration and production where he was Head of Automation and Control. He is now a Director of C&C Technical Support Services Ltd, which specialises in the application of the IEC 61508 standard, and he was a founder Director of the CASS Scheme Ltd for conformity assessment to IEC 61508. He chaired the UKOOA working group that produced the UKOOA Guidelines for Instrument-based Protective Systems, as an offshore sector interpretation of IEC 61508. He has a BSc. and MPhil in Control Engineering, is a Member of the IEE and currently chairs the Institute of Measurement and Control Safety Panel.

Contact Details:

Clive Timms

Technical Support Services Ltd

Strathayr

Rhu-Na-Haven Road

Aboyne, Aberdeenshire, UK, AB34 5JB

Tel: + 44 (0) 1339 886618

Fax: +44 (0) 1339 885637

email: c.timms@ifb.co.uk

Web: http://www.silsupport.com