Alarm Management & Graphics Projects

Ian Nimmo

User Centered Design Services LLC

Introduction

No doubt everyone who has a DCS has encountered alarm management issues and User Interface overload. Why is that you may ask? Well, the DCS arrived in a market place that had enforced restrictions of alarms due to physical space limitations and an instrument panel that allowed pattern recognition of process changes. To do anything with raw alarms was almost impossible; the only feature found in the electro-mechanical alarm annunciator box was first-up alarm indication and the ability to suppress the alarm by removing the electronics from the box.

The DCS provided flexibility, including almost unlimited alarms, multiple types including bad process variable monitoring and a host of options from filtering techniques to relational dynamic alarm rationalization. Unfortunately the DCS came without any discipline, cost implications for adding alarms and no warnings. To be fair to DCS manufacturers even the very first version of the Honeywell DCS gave advice on configuring and prioritization of alarms, not too different to the latest guidelines, however, no one read it or implemented this guidance.

"Leadership is solving problems. The day soldiers stop bringing you their problems is the day you have stopped leading them. They have either lost confidence that you can help or concluded you do not care. Either case is a failure of leadership".
Author: Karl Raimund Popper - Topic: Leadership

The problem was compounded by the lack of leadership and ownership issue that still exists at many of sites. In the past, after process engineers specified process alarms and equipment engineers requested alarms for protection of equipment, control engineers working on the installation of the DCS added alarms based on what could be done, not what should be done. Operators demanded alarms based on ease of monitoring, trying to make up for deficiencies in the Human Computer Interface and loss of the big picture as the panel they had been so used to disappeared and was reduced to a 15 inch key-hole window to the process. Multi-disciplined "Process Hazard Assessment" teams conducting HazOps that added alarms to deal with deficiencies in the design. The result being a process plant that went from 150 physical alarms to 14,000 DCS alarms.

Anything that is wasted effort represents wasted time. The best management of our time thus becomes linked inseparably with the best utilization of our efforts.
Author: Ted W. Engstrom - Topic: Existence

Management has been reluctant to pay for re-design of the alarm management system and the Human Computer Interface (HCI) as they felt they had already paid for the design once and could not see justification in paying again. Management knows that bad design has impacted operators' performance, even to the point of demanding extra manning to deal with the flood of alarms that occur during every disturbance, and has caused minor incidents from operators missing critical information or through human errors due to stress and overwork. Unfortunately it often takes a big incident to force companies to re-address the issue (as in the Texaco Pembroke incident quoted in all the alarm management guidelines).

"How do you eat an elephant – one bite at a time?"

How do we resolve this problem? The answer is careful review of the causes we have just outlined and starts with clear ownership of the problem. Some sites have identified a clear custodian who has responsibility to measure, correct and manage the problem, while other sites have made a multi disciplined team responsible.

The key to success is to establish responsibility; success should be based on performance, which is not just performance in resolving the number of alarms but the effects, the improvement to operator's jobs and the impact to the running of the plant.

Resolving any problem that involves costs, people and other resources should mean "Project Management" however, because of the lack of ownership, lack of accountability, and no performance expectations, alarm management projects rarely start with formal Project Management. A lot of alarm management projects start and fail due to poor understanding of the scope of the problem, lack of resources, and money, loss of momentum, and no identifiable return on investment.

Most managers get frustrated with engineers because engineers don't define the problem and the real cost implications to do the project correctly. They attack the problem without a plan and wonder why they don't get the support of the organization to address all the issues that surface.

We have seen many Alarm Management projects that are started by a frustrated manager who engages a Control Engineer to resolve the problem. The initial thoughts are the problem is limited to control system configuration and a few sit down discussions with the operators will resolve the problem, similar to other control system problems. Soon the control engineer realizes that he cannot make the decision to remove an alarm as some operators will not part with any, even though during a disturbance they get negative benefits from the alarm system.

The control engineer then involves a Process (Chemical) Engineer but together they are just overwhelmed by the size of the problem and the complexity. The control engineer reads recent articles on the subject and discovers that they need statistical tools to better understand what is happening within their alarm system.

The first information they get from the recently obtained tools (trial software) is a list of frequency of alarms and that just 12 alarms in the system produced 53% of the activations in the system and one particular alarm was responsible for 123 alarm activations in a 4 hour period.

This is known as the top 10 bad actor list. The two engineers discovered that just fixing those 12 alarms was a very challenging and time consuming task. Some of the alarms required physical instrumentation modification, some needed configuration changes which would involve better understanding of why the alarm existed and what the limits should be, when the alarm is not useful and should be suppressed and that some of the alarms were just not necessary, some required the alarm priority to be changed, which done against just 12 of the total configuration of thousands of alarms would still have little effect.

This little exercise demonstrated to the engineers that to solve this alarm management problem would require a multi-disciplined team, some members permanently on the team and others part-time as required such as rotation equipment specialists, PLC experts and other Subject Matter Experts (SME's). The experts would be specialized in equipment, safety, environment or process technology as these are the main reasons the alarm exists. The tool would be required throughout the project and as part of the life-cycle of the alarm system so a capital project would have to be justified to purchase the tool.

The full-time team would need a process engineer, control engineer, a supervisor with good experience of the plant and a couple of knowledgeable operators. Dealing with the first 12 alarms the team discovered they would need up-to-date documentation including accurate P&ID diagrams, DCS data sheets, PLC Ladder Diagrams, Procedures, etc. Often the team needed to call on other resources to either validate the documentation or find missing information, which introduces costs, delays and resource planning issues.

The team would also discover that initially they could only get through a handful of alarms per day and with the documentation checks, new documentation generation, management of change, realistically they could only review between 15 and 30 alarms per day. One site could only do 5 alarms per day because of other commitments and would take the team over three years just to get through the current alarm database.

This long term resource dependent type project with initial capital expenditure will require formal project management which is critical to success and should start with a program that addresses the following elements:

- Who owns the problem?
- What is the purpose of the project?
- What results should it achieve?
- What resources are needed?
- The site’s readiness to change existing practices
- Project Statement
- Project Objectives
- Work Breakdown Structure (WBS)
- Resource Requirements
- Project Management discussion
- Performance expectations

"When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meager and unsatisfactory kind." Lord Kelvin

Companies have recently put a lot of effort into resolving alarm management issues and the best of the best are doing this by first measuring a site’s performance against a benchmark. This benchmark is derived from the EEMUA 191 Guidelines document and has been broken down by one company into five classifications of performance:

1. Overloaded
2. Reactive
3. Stable
4. Robust
5. Predictive

Doing a gap analysis at the outset of the project can help the site understand where they are compared to where industry states they should be? It also provides the opportunity to set goals and milestones for resolving the problem. Moving from overloaded to stable may be a first phase. This phase may involve simply resolving alarm configuration problems, removing duplications, and continuously resolving top 10 bad actors that are contributing to the majority of the alarm floods. Moving from stable to robust may be a separate phase that requires additional capital to resolve issues. Some sites may choose to never get to predictive, or, to make it a stretch goal.

This philosophy is dependent on how bad a problem a site may have, how determined they are to resolve the problems and this comes back to those initial project management questions. What’s the purpose of the project and what results are to be achieved? Some companies just want to deal with the initial problem while others strive for a best practice solution, others may have had a dictate from a regulator which determines the goals. No one wants an overloaded system. This has motivated a company to do something about the problem. They don't want a reactive system. This is often where some companies start from as the alarm system is not useful during disturbances. A stable system is defined as reliable during normal operations and provides some advanced warning of a disturbance. It still has problems during a big disturbance.

This phase is often the first milestone for the project team and to address the next phase of alarm issues will require another level of design often involving dynamic alarm management strategies and additional software. After all this investment, companies want to see a return in time and resources so achieving a robust design may be the end goal. Few companies achieve the predictive performance, but the best-in-class do. Judging by the quality of technical papers and the content of papers from BP they have clearly demonstrated that predictive performance and the EEMUA Guidelines performance standard is achievable.[1]

"I conceive that the great part of the miseries of mankind are brought upon them by false estimates they have made of the value of things". - Author: Benjamin Franklin

"The rabble estimate few things according to their real value, most things according to their prejudices". - Author: Cicero (Marcus Tullius Cicero)

Estimating the cost of an alarm management project can be difficult for an engineer who has never done it before. The good news is many have done it before and there is a wealth of knowledge and learning at our disposal. Some common costs often not estimated at the beginning of a project are:

- The cost of hiring a Subject Matter Expert (SME) to get the project on the right tracks and educating the whole team on best and industrial practices. It is very expensive to start and fail and start an alarm management project over again.
- The costs for tools such as the PAS Inc. AMO Suite. This is a necessary investment to analyze any alarm database and identify problems, document solutions and implement change.
- The internal cost of multi-disciplined resources to participate in workshops, alarm objective analysis, DCS configuration changes, modifications to PLC databases, changes to SIS's, fixing instrumentation and plant equipment, updates to training manuals, procedures, MOC systems, enhancements to HCI, and process changes.
- The existing technology may not be capable of achieving predictive performance; hence, the company may have to invest in new application

[1] Horses for Courses – A Vision for Alarm Management, by Donald Campbell Brown, BP Upstream Technology Group (UK) – IBC 2002.

software to do dynamic alarm handling and State Estimation prediction technology.

"There are four kinds of people, three of which are to be avoided and the fourth cultivated: those who don't know that they don't know; those who know that they don't know; those who don't know that they know; and those who know that they know".

Getting the right people on an alarm management project is essential to success; unfortunately experts are always in high demand, especially on progressive process plants. Therefore, using people effectively should be part of the project plan. Some members of the project team may be full-time but others will be called on for advice.

One alarm management project failed due to lack of knowledge and the project team's inability to read PLC Ladder Logic. A large number of alarms were originated from the PLC and communicated to a DCS for presentation to operators. The team was not able to determine the source of the alarm or understand its objectives. No one had identified the need for a PLC specialist to be part of the team. This limited the team's ability to address the real issues, it extended the time to achieve anything, and caused frustration within the team until it lost energy and gave up.

Another team failed because of lack of correct information and knowledgeable personnel. A DCS manufacturer was employed with a local engineer to resolve alarm management project. Unfortunately the P&ID drawings given to the vendor were out of date and equipment that is currently out-of-service was not flagged. The DCS database did not reflect plant changes and as modifications to the plant occurred the tags were re-used without changing the process descriptors. The vendor used their budget on rationalizing and resolving inconsistencies before they realized they had focused on resolving problems with out-of-service equipment. Any of the plant operators working on the plant would have picked up these errors.

Time is the Rider that breaks youth. - Author: George Herbert: Jacula Prudentum

Most alarm management projects have some degree of success, due to the size and nature of the problems, but few achieve the initial goal of resolving all the alarm management problems. This is often caused by poor estimation of the time required to fix this type of problem and the complexity of the knock on effects of alarm management such as the implications to other systems such as procedures, training, HCI, etc.

Some of the classic examples of good alarm management projects such as the Woodside project in Karratha, Southern Australia have been implemented over the last five years and they still have work to do. In alarm management there is no such thing as a quick fix. Different companies address the problems from different angles. Some start fresh and add alarms based on Objective Analysis to a new empty database. Others work with the problem database reducing it slowly over time, first by removing duplication, then unnecessary alarms working at a rate of about 30 alarms per day for an experienced multi-disciplined team.

Some companies do not understand that alarm problem resolution is an iterative process and involves data collection, and analysis, fixing physical problems, identifying and eliminating unnecessary alarms, making enhancements to required alarms, creating and updating documentation, performing management of change (MOC) review, implementing, testing and starting over. These enhancements may consist of filtering, shelving, suppressing, or changing alarm type from deviation to physical or visa versa. Good alarm management projects start by focusing on the end or life-cycle aspects, with a goal of transitioning to a new way to maintain good alarm management practices.

Failure comes only when we forget our ideals and objectives and principles.
Author: Nehru - Topic: principles

Some of the reasons for failure of alarm management projects include:

- Having overly modest goals
- Leaving escape hatches for those who miss goals
- Valuing explanations as highly as results
- Providing no real consequences for performance levels
- Having too many goals
- Having vague or un-measurable goals
- Lacking clear accountability
- Having weak or nonexistent work plans
- Allowing confused decision-making processes
- Letting change become a crisis, not a routine
- Having low expectations
- Letting each area go its own way
- Conducting infrequent or ineffectual program reviews
- Following old, familiar routines
- Being “too busy” to be thoughtful
- Impulsively trying one thing, then another
- Overlooking the views of others

Based on Why Consultants Fail - High impact Consulting – Robert H. Schaffer

Courage is what it takes to stand up and speak; courage is also what it takes to sit down and listen. – Winston Churchill

Common problems that lead to failure to resolve alarm management issues:

- Lack of state of the art knowledge and reluctance to pay for a Subject Matter Expert (SME) upfront
- Lack of understanding of the real problem
- Lack of ownership

- No formal Project Management
- Clients not being ready to change existing practices
- Setting unrealistic goals
- Unrealistic estimate of costs and resources and planned budget
- Not getting the right people at the right time
- Using inaccurate out-of-date information
- Unrealistic time expectations
- Focus on project and not the life-cycle aspects
- Don't reward success and accept failure

This list is not extensive but represents some of the main issues associated with failed alarm management projects. Successful projects have a clear alarm philosophy that is well documented and understood by all disciplines and has a good understanding of the EEMUA Guidelines even if you don't agree with all of the guidance. I believe the most successful projects are ones that have a clear understanding of the size and types of problems the team will encounter, that is established on ROI and is goaled to solve the problem once and for all time. At the end of the project the initiating project manager can see a difference in the day to day life of the plant. Equipment runs better, incidents are dramatically reduced and production targets are consistently achieved and the only alarm that sounds is one that requires an operator to take action.

User Interface Design

Schematic Design Methodology

We provide an overview of our methodology and describe the benefits of following our approach as well as provide a typical consequence if a key step is skipped.

How we approach graphics development

There are fundamental differences between our approach to graphics development and the approaches employed by graphics implementation providers. Our approach is firmly based on Human Factors design principles and involves more than simply passing P&IDs to the graphics provider for implementation. Our methodology contains the following nine key steps, with the end goal of providing simple, coherent and usable graphics to the client that will enhance operator performance.

1. Define Information Requirements
2. Create a Graphics Style Guide
3. Create a Graphic Object Library
4. Create Display Sketches
5. Conduct Operations Design Review
6. Conduct Implementation Design Review
7. Revise and Document Display Design
8. Conduct Quality Control of Implementation
9. Evaluate Usability Using Operators in a Simulation/scenario-based Approach

10. Enhance Display Design

Define Information Requirements:

This step is the key to our approach and is, in the end, what helps to set our designs apart. In this phase of the design process, we aim to understand the system being run, to the point of knowing what equipment and which phases of operation are sources of difficulty for operations teams.

We spend time interviewing operators to understand the environment and the issues they face as well as conduct interviews with engineering and support staff to complete the operations picture.

The result of the interviews is a firm understanding of the key operational relationships that reveal the dynamics of the system being operated, as well as the practical issues facing operations on a daily basis. The information obtained in these interviews provides the content required in the operating graphics. This allows us to design graphics for operators that provide the right information at the right time.

Understanding the content required of a graphic display is a fundamental design component that is often either completely overlooked or casually attempted, resulting in graphics that are not useful to operations and, in some cases, the graphics pages are completely ignored.

Create a Graphics Style Guide:

The purpose of the document is to provide guidance that will define the user interface and enable consistent presentation of information, which will improve the overall performance of the operator with the DCS system. A style guide is written to support the technical, operational and cultural requirements of the plant.

Topics may include: workspace management, the use of color, text sizes, line styles, equipment characteristics and the presentation of alarms. This is extremely important in Centralized Control Rooms and allows operator cross training of areas.

When this step has been overlooked, the result is a set of graphics pages that are not cohesive and are full of inconsistencies, ultimately leading to degraded operator performance.

Using a Graphics Object Library

The development of graphics is simplified by using a Graphics Object Library, which ensures consistency in the design and ease of use for operators doing complex cognitive tasks.

Some of the objects are simple and are provided to complete the object library set using the style of graphics we recommend from a human factors and cognitive processing perspective.

Other objects are more complex but are designed to provide the operators with all the critical information at a glance, thus improving their ability to process large amounts of information more effectively. These objects are valuable tools for normal operations as well as during upset or abnormal situations.

We have also found that by implementing these objects in the context of graphics specifically designed to support the tasks as well as the system, the overall number of graphics pages required has been significantly reduced.

The operators are still provided with the data and information they need, but are not required to call up several graphics pages to see the complete picture.

Object Libraries may be obtained with the DCS Control System, developed by the user or they maybe obtained from a third party graphics developer, they come in two forms a Visio/PDF specification or as a Visual Basic Code, Active X Controls. We provide both of these and they are designed to be application specific and ASM® Compliant.

Create Display Sketches:

Our design team has been formally educated in Human Factors engineering that allows us to turn the information requirements gathered in the first phase of our approach into graphics designs that are intuitive to operations staff. We achieve this end goal by incorporating graphics concepts that support the way people perceive and process information. Understanding and aiding human limitations related to information perception and processing in abnormal situations, frees up the operator's mental resources that can be better put towards recovery tasks.

It is for these reasons that our graphics take on a form that is atypical of P&ID graphics pages. We make minimal use of digital values and maximize the use of graphics that aid pattern matching so that operators can make quick determinations about the state of a system without taxing their memory resources.

At first glance, our graphics designs might seem odd because they are different. A second glance reveals their useful and intuitive design. Part and parcel to our design philosophy is providing graphics within a structured hierarchy to aid an operator when solving a problem.

Our hierarchy consists of four levels of graphics, which we have labeled Type 1 to Type 4. Figure 4 below is a graphical representation of the hierarchy for your convenience.

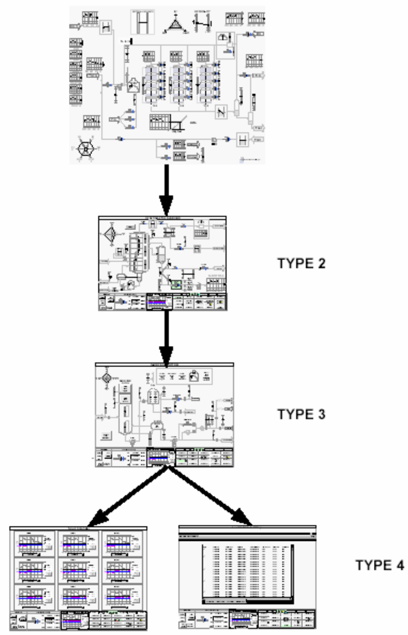


Figure 1: Example of the display hierarchy employed in our methodology

Humans have very definite, ingrained, steps to solving a problem. First they attempt to look at the bigger picture and then they drill down to the part of the process that is the source of the problem. Unfortunately, the bigger picture was lost when the panel board was replaced with the various incarnations of the DCS.

In our design scheme, we endeavor to return the bigger picture to the control room in the form of overview displays that provide key information to the operator related to their entire span of control. The overview, or Type 1, displays reside in the top level of the hierarchy below.

The area, or facility, overviews form the basis of the Type 2 displays. The purpose of the Type 2 display is to provide the operator with a means of quickly determining the health of a major system within their span of control. In addition, we provide dedicated task oriented displays at this level of the graphics hierarchy to allow operations to quickly detect, diagnose and recover from a pending situation.

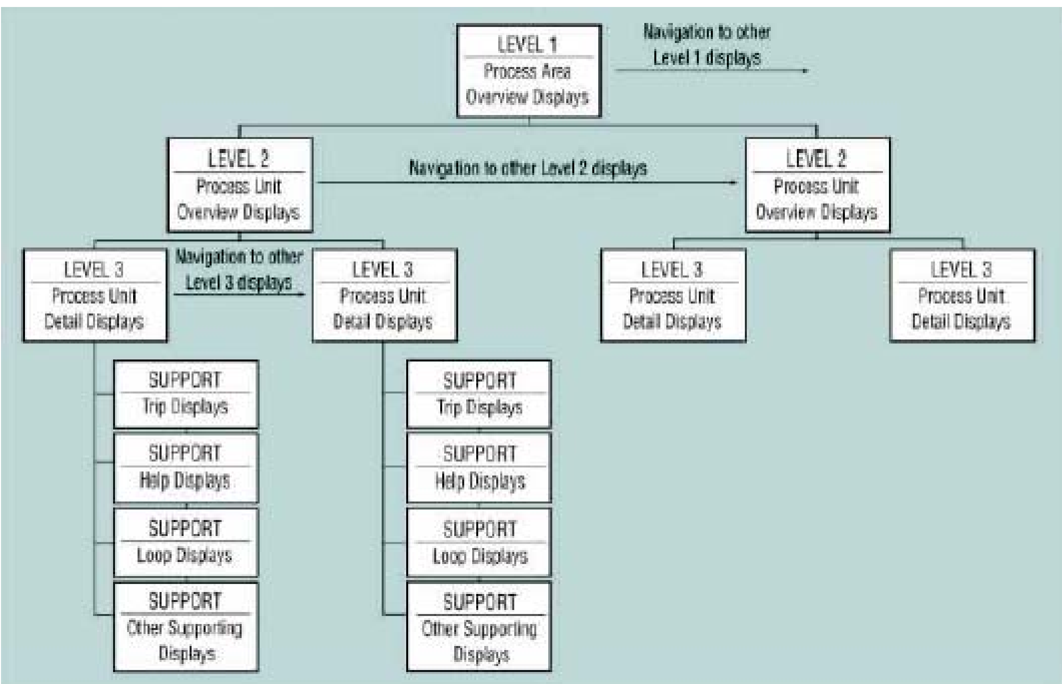
The necessity for the number of task displays is directly a result of the phase 1 Information Requirements analysis that we perform. Examples of task-oriented Type 2 displays include, but are not limited to, start-up and shutdown displays.

Almost all graphics, that are implemented in refineries worldwide, reside in our third level of the display hierarchy, referred to as Type 3 displays.

The purpose of Type 3 displays is to provide detailed information not displayed on the Type 2 displays. Type 3 screens are detailed process displays that provide detailed views of sub units, equipment, related controls and indications.

These displays should be used for routine operations, such as switching of pumps, starting blowers, opening drain valves and so forth. Type 3 displays will also be used for detailed diagnostics in interventions that are not time critical.

The last type of display within our hierarchy is the Type 4 display. The main purpose of Type 4 displays will be to provide additional, or miscellaneous, information that will be useful for operating a particular section or piece of equipment within a unit. Type 4 displays do not contain control functions. Typical examples of Type 4 displays include: Alarm summary display; Procedure and Help displays; Trend displays and System diagnostics.



Conduct Operations Design Review:

The purpose of this phase is to review the initial design sketches with operations to ensure the validity of the design, to begin to obtain operator buy-in to the graphics and to obtain operations comments that will begin to finish the design. If this phase of the process is overlooked, the result is incomplete graphics that may be incorrect. The overall performance of the graphics, operator ownership and familiarization are greatly enhanced during this step.

Conduct Implementation Design Review:

In this step, the graphics that have been reviewed by operations representatives are then passed onto the implementation team to determine if there are any potential implementation issues with the designs. It is a checkpoint in the process that ensures the most efficient design-to-implementation process as it limits the amount of artistic liberty employed by implementation team. Any implementation issues that result in redesign are most effectively handled at this point in the process and therefore minimize the cost and effort related to re-work on graphics.

Evaluate Usability Using Operators in Simulation/Scenario-based Approach:

Once the graphics have been implemented in the system, they are evaluated as a group in certain key mocked-up situations that provide a final source of feedback into the design. This is performed with real operators performing relevant tasks with the system they will be operating, thereby affording observation of issues with the interface that even the operators might not be aware that they are having. The cohesiveness of the graphics as a whole, when performing routine tasks or recovering from abnormal situations, is assessed and any necessary adjustments to the graphics are determined.

Enhance Display Design:

This is the final step in our process and it serves as a point at which any minor adjustments determined by the above evaluation phase are made as well as all documentation, such as the design specification and associated training materials, is finalized.

Ian Nimmo is President and a founder of User Centered Design Services an ASM Consortium affiliate member and an ASM service provider. He served 10 years as a Senior Engineering Fellow and a founder and Program Director for the ASM Consortium for Honeywell Industrial Automation & Control, Phoenix, before joining Honeywell; he worked for 25 years as an electrical designer, instrument/electrical engineer, and computer applications manager for Imperial Chemical Industries in the U.K. He has specialized in computer control safety for seven years; he has extensive experience in batch control and continuous operations. He developed control hazard operability methodology (ChazOp) during his time at ICI and has written over 100 papers and contributed to several books on the subject. He studied electrical and electronic engineering at Teesside (U.K.) University. He is a member of the Institute of Electrical and Electronic Incorporated Engineers, and a senior member of the Instrument Soc. of America.

References:

Andow, Peter, "Alarm Performance Improvement During Abnormal Situations," HAZARDS XV: The Process, Its Safety, and the Environment: Getting it Right, Institute of Chemical Engineers, Manchester, UK, April 2000.

Campbell Brown, D., "Horses For Courses - A Vision For Alarm Management", Paper presented for IBC 2002

Campbell Brown, D. and O'Donnell, M, "Too Much of a Good Thing?–Alarm Management Experience in BP Oil, Part 1: Generic Problems with DCS Alarm Systems", Paper Presented IEE Colloquium on Stemming the Alarm Flood", London, 1997.

Fitzpatrick, B., "Alarms in the Real World", Paper Presented at Honeywell North American Users Group Meeting, Phoenix, 2001.

Mattiasson, C., "The Alarm System from the Operator's Perspective", Paper Presented at IEE People in Control Meeting, Bath, UK, 1999.

Metzger, D. and Crowe, R., "Technology Enables New Alarm Management Approaches", Paper Presented at ISA Technical Conference, Houston, TX, 2001.

Mostia, B., "How to Perform Alarm Rationalization", Control, August 2003.

Nimmo, I., "The Importance of Alarm Management Improvement Project",   Paper - Presented at ISA INTERKAMMA, Germany1999.

Nochur, A., Vedam, H. and Koene, J., Alarm Performance Metrics, Singapore Honeywell Singapore Laboratory, 2001.

O'Donnell, M. and Campbell Brown, D., "Too Much of a Good Thing?–Alarm Management Experience in BP Oil, Part 2: Implementation of Alarm Management at Grangemouth Refinery", Paper Presented IEE Colloquium on "Stemming the Alarm Flood", London, 1997.

PAS (Plant Automation Services) The Cost/Benefit of Alarm Management, Houston, TX: Plant Automation Services, 2000.

PAS (Plant Automation Services), White Paper: Alarm Management Optimization, Houston, TX: Plant Automation Services, 1998.

Smith, W., Howard, C. and Ford, A. (2003), Alarm management – priority, floods, tears or gain?, www.4-sightconsulting.co.uk: 4-sight Consulting.