Executive Summary

In 2005 the National Transportation Safety Board concluded that an effective alarm review/audit system will increase the likelihood of controllers appropriately responding to alarms associated with pipeline leaks. This paper looks at the pipeline industry in the broader context of process industry alarm management and how the best practices of the process industry apply to the pipeline industry.
# Table of Contents

- **Executive Summary** ........................................................................................................... 1
- **Background** ....................................................................................................................... 4
- **History** ............................................................................................................................... 5
- **Definition of Alarm** ............................................................................................................. 5
- **Alarm Management Best Practices** ..................................................................................... 5
- **Alarm Philosophy** ............................................................................................................... 5
- **Benchmark and Performance Audit** .................................................................................... 6
- **Rationalization** .................................................................................................................. 7
- **Bad Actor Clean Up** .......................................................................................................... 7
- **Rationalization** .................................................................................................................. 7
- **Dynamic and State-Based Alarming** .................................................................................. 8
- **Implementation** ................................................................................................................ 8
- **Continuous Improvement** ................................................................................................. 8
- **Manage Change and Corporate Culture** .......................................................................... 9
- **SCADA Perspective** .......................................................................................................... 9
# Table of Figures

| Figure 1: | Alarm Tree Map | ................................. | ........................................................................................................ | 6 |
| Figure 2: | Alarm System Performance Levels | ........................................................................................................ | ................................................................. | 7 |
Background

On April 27, 2006, before the Subcommittee on Energy and Air Quality, Bob Chipkevich, Director of the US Office of Railroad, Pipeline and Hazardous Materials Investigations, stated, "The study found that an effective alarm review/audit system by operators would increase the likelihood of controllers responding appropriately to alarms associated with pipeline leaks. The Board (meaning the National Transportation Safety Board (NTSB) recommended the PHMSA (Pipeline and Hazardous Materials Safety Administration) require pipeline companies to have a policy for the review/audit of alarms....." The questions plaguing a lot of pipeline operators are, "What does this mean to me?" and "What are the best practices for alarm management?" First let us look at a little history regarding alarm management, and this will help determine where to look to find answers to these questions.

Mr. Chipkevich’s testimony was a summation of the NTSB safety study released in 2005. This study looked at 13 hazardous liquid line accidents from 1992 to 2004 and identified some aspect of the SCADA system as contributing to the severity of 10 of these accidents. One could conclude that alarm management is something relatively new, but in 1992, Occupational Safety & Health Administration (OSHA) formalized the Management of Change (MOC) as one of the 14 elements of its process safety management regulation. Shortly thereafter, the US Office of Pipeline Safety issued an advisory suggesting that pipeline SCADA systems be subjected to MOC procedures. It was thought that all changes in the process control system should fall under MOC. Generally speaking, it was viewed that changes to limit values, could lead to safety problems. Indeed, there were several incidents to support that view. Adding alarms appeared to be a benign effort. However, the cumulative effect of adding alarms leads to alarm floods and a burden on the SCADA controller.

On December 23, 2003, Advisory Bulletin ADB 03-09 was published in the Federal Register and stated that a good practice for pipeline owners and operators was to periodically review their SCADA system configurations, operating procedures and performance measurements. Alarms are part of the configuration, and alarm response is part of the operating procedures. Another question to puzzle the pipeline operators: how do you measure the performance of the alarm system?

The NTSB safety study reported that controllers viewed the alarm as the most important safety feature of the SCADA system, yet some companies are experiencing rates of 100 alarms per hour. Incident investigations have shown controllers to miss alarms, respond incorrectly to alarms and misinterpret specific alarms as being insignificant. Also, alarms have been incorrectly configured, inhibited and had inappropriate alarm thresholds. What we find when we dig into the questions is that alarm management is not new, but as a result of the NTSB safety study, there is a renewed awareness of alarm management in the pipeline industry. One needs to look outside the pipeline industry to find the answers to “What does this mean to me?” and “What are the best practices for alarm management?”
History
Looking outside the industry, we find that the modern day context of alarm management started to form around 1988 with the creation of the ASM consortium. This was followed by a great interest in:

- 1988+ ASM Consortium
- 1997 FDA 21 CFR Part 11
- 1998 HSE Studies
- 1999 EEMUA 191
- 2001 Norwegian Petroleum Directorate YA-710/11
- 2003 NAMUR NA102
- 2005 National Transportation Safety Board Safety Study
- 2006 API/AGA Alarm management projects
- 2007 ISA SP18.02, Management of Alarm Systems for the Process Industries
- 2008 ANSI Adoption of ISA
- 2009 Standards Australia

Today, we find the EEMUA (Electrical Engineering Manufacturers Users Association) 191 document to be the de facto world standard. Within this recommended practice are a series of measurements or key performance indicators that take human capabilities into account. It is this document that companies benchmark, audit and review their alarm systems against. It is these published KPIs that provide the understanding for the pipeline industry to develop a policy for the review and audit of alarms as recommended in the NTSB safety study. The ISA SP.02 committee’s work will build upon EEMUA even further and is scheduled for release in 2007.

Definition of Alarm
Before examining alarm management best practices, we need to define what an alarm is: An audible or visible means of indicating to the controller an equipment or process malfunction or abnormal condition requiring a response.

An alarm has three basic functions:
- notifying the controller of an abnormal change;
- communicating to the controller the nature of the change and possible causes;
- directing the controller to take appropriate corrective action.

Keep in mind as we look at best practices that an alarm must not be expected and must require a controller action.

Alarm Management Best Practices
Alarm Philosophy
The NTSB safety study has a section titled “alarm philosophy,” but the section does not detail best practice as it has been adopted in the process industries. The alarm philosophy or technical requirements and typically done at the pipeline or workstation level, although some organizations develop a corporate philosophy with appendices for the specifics of each SCADA station. The alarm philosophy documents the management process encompassing the alarm management program as well as the actual alarm creation and handling guidelines. Typically the alarm philosophy will cover the alarm management review process, the management of change control, roles and responsibilities, SCADA specifics, alarm setting guidelines, alarm handling criteria, system monitoring, testing, documentation control and training. This document will define the methodology for setting alarm priorities and alarm thresholds. It becomes the cornerstone of the alarm management program as it develops into a guideline, rule book, interpretation guide and the center for rationalization.

Successful organizations have found that the process of creating the alarm philosophy can be as valuable as the document itself, as it brings all the views, opinions, and methodologies of all employee resources into a common framework. It helps standardize the configuration across multiple lines, especially in a situation where pipelines have been acquired rather than built by the operating company.
Benchmark and performance audit

One of the recommendations of the NTSB safety study was to “require pipeline companies to have a policy for the review/audit of alarms.” This alone is a good reason to complete an audit of alarms, but the benchmark and performance audit may be done for several other reasons as well:

- understand where you are relative to best-practices guidelines
- compare your pipelines to industry best practices
- analyze your current system performance to determine problem areas
- create an informed path forward
- help justify business case
- show due diligence

The benchmark and performance audit involves an audit of all management processes as well as actual alarm performance. During the alarm performance audit each of the KPIs defined in the alarm philosophy, which may match those of EEMUA 191 where they are applicable, are calculated and interpreted. To complete the alarm performance audit, the alarms and events must be historized in a fashion that allows for alarm and event analysis. The analysis is generally completed using software tailored to the measurement criteria suggested in EEMUA 191.

Figure 1: Alarm Tree Map

The representation of the final interpretation may take many forms such as the tree map shown in figure 1, where the alarm performance of an entire pipeline system may be visualized on one screen.

Alternatively, the audit may be summarized by classifying the facility as D.C. Campbell Brown of British Petroleum proposed in his paper “Horses for Courses – A Vision for Alarm Management” and as shown in figure 2.
Rationalization

Bad Actor Cleanup

During a benchmark and performance audit, bad-acting tags will make their presence known. At the outset of rationalization, it is good to clean up these tags, which could contribute up to 50% of the controllers’ daily alarm load. Quick success is helpful in gaining operational support for the alarm management endeavor. These bad actors are the alarms that are chattering. They are redundant with other alarms, alarms that have no operational action associated with them or have limits in the normal operating range. Do this and your controllers will thank you.

Rationalization

The classic method of rationalization involves a team of people from operations and engineering, gathered together with an impartial facilitator to methodically review alarm settings on each alarmable SCADA tag. The key to successful rationalization is preparation. Preparing for an alarm rationalization can be onerous and time-consuming. It requires the following actions:

1. Understand the alarm capabilities of the SCADA. Specifically, one must be able to answer:
   - What parameters drive alarm generation?
   - What priority values are available? Which priorities are audible / visible?
   - What message/alert capabilities exist?
   - How do deviation alarms work?
   - How would I count the number of alarms configured on tag? EEMUA 191 has guidelines on configuration numbers.

2. Get a SCADA database extraction. Ensure you understand how to categorize all tags into a pipeline hierarchy (pipeline\segment\unit).

3. Create a master alarm database.

4. Ensure the necessary personnel will be participating. Based on tags per pipeline, segment, and unit, accurate estimates can be derived to schedule personnel’s time. Generally speaking, the following resources are required:
   - experienced SCADA controller and/or shift supervisor
   - pipeline hydraulic and/or station process engineer
   - meeting facilitator
   - SCADA engineer for the first few days, especially if you are not experienced with the SCADA system
5. Ensure that logistics are looked after. You will need a proper meeting place, supporting documentation and infrastructure that enables the process to be efficient. Once the preparation is complete, review the rules of engagement:

- What conditions allow for an alarm?
- How are severities classified and determined?
- What are the time-to-respond categories?
- How are priorities determined?
- What alarm limits are the controllers allowed to alter? (e.g.: priority “3” only?)
- Are alerts and/or messages available?

With the preparation complete, it is time to start the rationalization. Review each alarmable tag on a loop basis, determining the time to respond, severity, limit, causes, initial responses and corrective actions. Set priorities and alarm limits based on these decisions, then document results and record follow-up items and logic opportunities (dynamic alarming/cut-outs).

**Dynamic and State-Based Alarming**

With classic rationalization complete, dynamic and state-based alarming can be investigated. This is not a simple activity and takes a solid understanding of the operational and control philosophies of the facilities during all relevant states. During this stage you:

- identify time of alarm floods
- determine how to sense the initiating event
- identify tags that alarmed during the flood
- determine what is normal during the event
- list problems
- list available tags
- engineer new alarms
- build new alarms
- remove old alarms
- suppress non-relevant alarms

Care must be taken to test the logic prior to implementation to ensure unsafe conditions are not generated as a result of alarm suppression.

**Implementation**

Implementation is the practice of changing the control system configuration to match the decisions made during alarm rationalization. This is best implemented in two phases:

1. Implement static settings as documented in the master alarm database.
2. Implement suggestions for control system logic to consolidate alarms.

Run a discrepancy report. If the list is manageable, simply implement the SCADA settings that do not match the engineered settings. As the changes are made in the SCADA, the discrepancy list will get smaller and smaller until it is complete.

**Continuous Improvement**

Alarm management has a lifecycle and is not a one-time project. Continuous performance monitoring helps to identify new opportunities for improvement, such as dynamic alarm strategies. It identifies new opportunities to optimize the alarm system, and alarm floods provide opportunities to better refine dynamic suppressing strategies.
Manage Change and Corporate Culture

Organizations successful at alarm management integrate the practices into the workflow to optimize performance over the long term. Good practice ensures that problems that do arise are identified, resolved and documented in a timely fashion, providing:

- audit trail of all changes to the SCADA
- documentation of reasons for changes
- sustained and improved alarm system performance
- approval of all alarm changes
- a knowledge base from experienced personnel

SCADA Perspective

Is the pipeline SCADA system different than the DCS system in a process facility? Technically, the capabilities of the two are very similar. There are differences in communication methods, scan rates, RTUs vs. IO modules, etc., but from the controller’s perspective, both systems provide a window into their operating environment through which they monitor the pipeline, control it and respond to abnormal situations. From an alarm management perspective, one must consider the following:

- a pipeline controller may operate more than one pipeline simultaneously. These may be interconnected or totally independent. They may carry dramatically different compounds which have vastly different environmental and safety concerns. The consequences of events can be significantly different, resulting in the need for different criteria for alarm priorities.
- for many pipeline controllers, the pipeline includes compressor stations, underground storage facilities, perhaps LNG or propane-air peaking stations, straddle facilities, gate stations and hubs. The controller may be called upon to be a station operator as well a pure pipeline controller.
- a pipeline controller may operate without storage in a single-source environment, so a shutdown may impact other players where there is no alternative source. Essential services play heavily when setting alarm priorities.
- at a micro level, the pipeline controller has no controller action for many typical alarms associated with rotating equipment. Should that equipment fail, however, the controller must respond to the impact of the failure on overall pipeline operation. The pipeline controller may also be called upon to do remote shutdown of equipment or stations for particular situations.
- The pipeline controller operates facilities across vast geography with stations that are unmanned. These facilities may be subject to undesirable third-party intrusion and take time for field operators to get to.
- many actions of the pipeline controller are to dispatch field operators, with no direct control ability available to the controller.
- due to varying communication methods there are often different latencies associated with different sites.
- pipelines tend to be subject to third-party damage at a higher rate than process facilities.

None of the above has any impact on the fundamentals of alarm management, but they all impact the approach. The consequences associated with an individual alarm affect the setting of priorities, and the distances involved can make for vastly different times to respond, especially where the dispatching of field operators is involved. Fundamentally, though, the principles of alarm management best practices are as valid for the SCADA application as for the DCS application.
"There are more things to ALARM us than to HARM us, and we suffer more often in apprehension than reality."

- Lucius Annaeus Seneca