API-1167 PIPELINE ALARM MANAGEMENT:
Understanding and Applying the New API Recommended Practice, and
Powerful Solutions for Nuisance Alarms

BILL R. HOLLIFIELD
Principal Alarm Management and HMI Consultant, PAS


Bill Hollifield

Introduction

Over the last several years, alarm management has become a highly important topic, and the subject of a number of articles, technical symposia, and books.

In December 2010, the API published *Recommended Practice RP1167: Pipeline Alarm Management* (referred to as "API-1167" herein). The regulatory implications of this document, as well as PHMSA 49 CFR 192/195 and the standard ANSI/ISA-18.2: Alarm Management for the Process Industries (referred to as "ISA-18.2" herein) will be examined.

In addition, the paper includes explanation of several practical and powerful techniques for solving the most common alarm problems. Widespread experience has shown alarm rate improvement of 60% - 80% can usually be achieved by properly addressing a small number of problematic alarms.

The New Regulatory Environment for Alarm Management

The most significant recent regulatory event involving alarm management was the June 2009 publication of ISA-18.2.

Dozens of contributors, from a variety of industry segments, spent thousands of hours participating over six years in its development. The author participated as a section editor and voting member of both ISA-18.2 and API-1167.

The issuance of ISA-18.2 is a significant and important event for process industries, including the pipeline industry. It sets forth the work processes for designing, implementing, operating, and maintaining a modern alarm system presented in a life cycle format. It is having significant regulatory impact.

API-1167 was issued 18 months after ISA-18.2 and the documents are very similar and intentionally non-contradictory. It is important to understand the impact of ISA-18.2 as a precursor to the discussion of API-1167.

ISA-18.2 is quite different from the usual ISA standard. It is not about specifying how some sort of hardware talks to other hardware or the detailed design of control components. It is about work processes of people. Alarm management isn't really about hardware or

software; it's about work processes. Poorly performing alarm systems do not create themselves.

ISA-18.2 is a consensus standard developed per stringent ANSI methodologies that are based on openness, balancing of interests, due process, and consensus. These make it a ***"recognized and generally accepted good engineering practice"*** *(RAGAGEP)* from the regulatory point of view. This is a very important aspect.

There are several common misconceptions about standards. Standards intentionally describe the minimum acceptable and not the optimum. By design, they focus on what to do rather than how to do it. Also by design, standards do not have detailed or specific how-to guidance. ISA-18.2 does not contain examples of specific proven methodologies or of detailed practices. The standard focuses on both work process requirements ("shalls") and recommendations ("shoulds") for effective alarm management.

Does ISA-18.2 Apply to You?

The focus of ISA-18.2 is on alarm systems that are part of modern control systems, such as DCSs, SCADA systems, PLCs, or Safety Systems. It applies if you have a controller that responds to alarms depicted on a computer-type screen and/or an annunciator.

This includes the bulk of all process industries operating today, specifically:

- Pipelines
- Petrochemical
- Chemical
- Refining
- Platform
- Power Plants
- Pharmaceuticals
- Mining & Metals

The reason for this commonality is that alarm response is really not a function of the specific operation being controlled; it is a human-machine interaction. The steps for detecting an alarm, analyzing the situation, and making a response are human steps in which there is little difference if you are making (or moving) gasoline, plastics, megawatts, or aspirin. While many industries feel they are different, that is simply not the case when it comes to alarm response. Many different industries participated in the development of ISA-18.2, recognized this, and the resulting standard has overlapping applicability.

Regulatory Impact

The regulatory environment is complex and overlapping for some industry segments. Many industries are clearly covered by the OSHA 1910.119 "PSM Rule", which makes a few specific mentions of alarms. The Pipeline industry is regulated by DOT-PHMSA, which pays much more attention to API Recommended Practices than it does to ISA Standards. However, understand that DOT/PHMSA regulators are aware of ISA-18.2.

The important thing is that regulatory agencies have general duty clauses and interpretations. As one example, consider OSHA 1910.119 (d)(3)(ii) which states, "The employer shall document that equipment complies with recognized and generally accepted good engineering practices (RAGAGEP)."

Codes, standards, and practices are generally considered as "recognized and generally accepted good engineering practices." In the OSHA interpretation letter to ISA, a National Consensus Standard, such as ISA-18.2, is a RAGAGEP, and OSHA recognizes ANSI/ISA S84.01-1996 as another example of such.

There exists a Memorandum of Understanding between OSHA and ANSI regarding these matters (see References).

Generally, a regulated industry can be expected to either comply with a RAGAGEP or explain and show that they are doing something just as good or better.

Recent PHMSA Regulations

In December 2009, PHMSA published regulations involving alarm management for pipelines. This was a year prior to the issue of API-1167.

The regulations are PHMSA 49 CFR Parts 192 (Gas Pipelines) and 195 (Liquid Pipelines), Pipeline Safety: Control Room Management Human Factors.

PHMSA regulations 192/195 require various alarm management practices be implemented, and mentions an alarm management plan as a required element.

PHMSA utilizes a different methodology than OSHA for the utilization of API Recommended Practices in their regulatory structure. DOT/PHMSA will specifically list API documents by name in their regulations. As examples, both 192 and 195 list portions of API-1165, "Recommended Practice for Pipeline SCADA Displays", as required, and 195 includes portions of API-1168, Pipeline Control Room Management.

Regulations 192 and 195 did not mention API-1167 because it was still in draft at that time. We fully expect the now-released API-1167 to be similarly incorporated and/or used in future PHMSA regulations and enforcement actions.

Figure 1 on page 9 is a cross-reference of 192/195 requirements and sources that can be used to prove compliance.

What is an Alarm Management Plan?

Regulations 192 and 195 refer to an "Alarm Management Plan" as a requirement. The first use of this term is in the PHMSA regulations; however, it is not defined.

In contrast, the term "alarm philosophy" has been around since the first works on alarm management began to be written in the mid-1990s. It refers to an operator's comprehensive document on how to create an effective alarm management system. Operators develop this document as part of an alarm improvement effort. It is one of the first steps in improvement. The term has well established meaning, and is used in ISA-18.2, *The Alarm Management Handbook*, and *EEMUA 191: Alarm Systems*.

Many operators have improved their alarm systems long before any PHMSA regulations were issued, and already have alarm philosophies.

A proper alarm philosophy covers all of the aspects of alarm management, including roles and responsibilities, rules and criteria for determining which things should be alarms, proper methods for determining and documenting alarm setpoints and priorities, rules for handling alarms, alarm system management of change, alarm system monitoring, and other work practice requirements around the alarm system. The API-1167 draft document has some examples of the content of an alarm philosophy. The ISA-18.2 standard makes some mention of the contents, and the committee is developing a technical report with more detail.

The recent PHMSA regulations now contain the term "alarm management plan." These regulations also have some very specific requirements. An operator should develop an alarm management plan for how to comply (at least minimally) with the regulation. A comprehensive alarm philosophy is part of the plan. If an operator has an existing alarm philosophy, they should check its contents vs. the requirements of the new PHMSA regulation, and fill any gaps and document any action items needed to comply.

Our opinion is that having an alarm management plan is met by having the following two items:

1. A comprehensive alarm philosophy document that meets the requirements and recommendations set forth in ISA-18.2 and API-1167.

2. A document specifying a plan and schedule for rationalizing the pipeline alarms, as well as a plan for the annual audit of alarm management required by PHMSA, API-1167, and ISA-18.2.

An Outline of API-1167
API-1167 has the following important content:

- Alarm definition and determination
- Purpose and use of alarm priority
- Safety-related alarms
- Other uses of the alarm system
- Alarm philosophy
- Alarm documentation and rationalization
- Determination and assignment of alarm priority
- Determination of alarm setpoint
- Recommended storage of D&R information
- SCADA control system alarm functionality and alarm design
- Alarm-related electronic records
- Alarm suppression and alarm shelving
- Leak or possible leak alarms
- Defined alarm design cases
- Roles and responsibilities
- Alarm handling
- Nuisance alarms
- Designed alarm suppression
- State-based or state-dependent alarms
- Alarm flood suppression
- Alarm audit and enforcement
- Special-purpose priorities and alarm routing
- Controller-adjustable alarms
- Controller alert systems
- Alarm audits and performance monitoring
- Alarm system performance metrics
- Alarm system key performance indicators
- Regulatory requirements for alarm system monitoring
- Management of change
- Regulatory requirements for change management

This paper will not deal with all of these, as there is no substitute for obtaining and understanding API-1167. However, a few of them are deserving of some commentary.

Alarm Definition and Determination:
API-1167 states that *"An alarm is a visible and/or audible means of indicating to the controller an equipment malfunction, process deviation, or other condition requiring a controller's response. The use of the term*

'alarm' in this recommended practice is referring to items meeting this definition."

"For alarms to have significance, the alarm system should be reserved for the indication of items that conform to this definition. Non-conforming information should be excluded from the alarm system, as it dilutes the importance of actual alarms. Such information can be more properly conveyed to the controller via a variety of other methods in the HMI (human-machine interface)."

This is a significant change from many common but poor practices of using alarms improperly! The SCADA system manufacturers make alarms so easy to configure and use that they are used for all sorts of inappropriate things. The alarm system is not to be used for miscellaneous status information. The importance of the alarm system is diminished when it is a combination of truly important alarms and a lot of trivial status change information. The trivia should be excluded from the alarm system.

Pipeline Safety-Related Alarms

The PHMSA regulation says the following: *"Alarm means an audible or visible means of indicating to the controller that equipment or processes are outside operator-defined, safety-related parameters."*

"Operator-defined safety related parameters" is not well-defined in the regulation. The astute reader, and particularly an engineer with a bit of a legal bent, may perceive a loophole here. Perhaps all of these regulatory alarm requirements only apply to the very few pipeline alarms that meet these narrow criteria?

Alas, this is not the case. PHMSA also notes that operators are required to monitor the content and volume of activity being directed to each controller since too many of the other alarms can overwhelm the controller and interfere with their detection of safety – related alarms.

So there is no escape from the need to monitor the overall performance of the alarm system, which has been a fundamental principle of alarm management for many years.

API-1167 provides several examples and ideas for determining which particular alarms are actually safety-related alarms.

A Special Note: Regulations 192/195 both require an operator to *"monitor the content and volume of general activity being directed to and required of each controller at least once each calendar year, but at intervals not to exceed 15 months, that will assure controllers have sufficient time to analyze and react to incoming alarms."*

We have heard of some consultants trying to convince pipeline operators that very expensive controller time-motion studies involving everything from telephone calls to bathroom breaks are necessary to comply with this requirement. We do not think so.

If you apply the proper principles of alarm management, then every alarm will be signifying a condition requiring the controller's response to avoid some sort of consequence. Every alarm becomes important. Therefore, alarm response becomes more important than, and is prioritized above, such activities as phone calls, reading email, meetings, and so forth. If the job description of the controller places alarm response above other activities, and your performance monitoring of the alarm system indicates acceptable alarm rates, then you should be covered. It is the phone calls and

office work that are shed when needed, not control of the pipeline and alarm analysis and response. Those are the top duties of the controllers.

Alarm Philosophy
You will need a comprehensive alarm philosophy. If you have not started, now is the time. API-1167 provides a fair amount of guidance as to contents.

Alarm Documentation and Rationalization
Alarm Documentation and Rationalization is a task that will require a significant amount of your time and resources to accomplish. It *will be* in your future. It involves reviewing all of your alarms to ensure they comply with the principles in your alarm philosophy. Certain information about each alarm must be documented. Literally millions of alarms have been rationalized in other industries, and there are very well-known techniques and solutions to accomplish this task efficiently and with minimum disruption. These methods are not highly detailed in API-1167..

SCADA System Alarm Functionality and Alarm Design
This is an informative section covering typical alarm functionality and issues with SCADA systems. It provides some good advice for configuring certain types of alarms.

Alarm Handling
This section covers some advanced methodologies and techniques for dealing with:

- nuisance alarms
- alarm shelving (this is manually-initiated alarm suppression that meets several important administrative requirements)
- designed alarm suppression
- state-based alarming
- special-purpose priorities
- alarm routing
- controller alert systems

Controller-Adjustable Alarms
It is an unfortunate, but common practice to allow controllers to adjust alarm setpoints at their individual whim. This leads to shift-based variation and a host of other problems. API-1167 recommends several very tight controls over this practice. It should be limited to a very few specific alarms, and the limits of adjustability documented. This will be a change for many.

Alarm System Key Performance Indicators
API-1167 has a section on recommended measurements and performance numbers for an alarm system. The table from ISA-18.2 is included.

The recommended analyses include:

- Average annunciated alarm rate per controller position
- Peak annunciated alarm rates per controller position
- Alarm floods
- Frequently occurring alarms
- Chattering and fleeting alarms
- Stale alarms
- Annunciated alarm priority distribution
- Configured alarm priority distribution

The PHMSA regulations require specific monthly identification of several aspects of safety-related alarms and other performance monitoring. These include:

- Monthly monitoring of points affecting safety that have been taken off scan, have alarms inhibited, generated false alarms, or have forced or manual values for durations exceeding those needed for

appropriate maintenance or operating activities
- At least annual verification of proper setpoints and descriptions of safety-related alarms
- Annual review of the alarm management plan
- Annual review of alarm system performance

Automated alarm analysis software with automated reporting capabilities is highly recommended to efficiently comply with this requirement.

Management of Change

API-1167 provides guidance regarding management of change of an alarm system. The MOC process should include:

- the scope of changes requiring the relevant MOC process (e.g., alarm additions, changes, or deletions)
- roles that have the appropriate rights to make alarm system changes
- what requirements should be met for evaluating change (e.g., risk assessment if appropriate)
- authorization of changes
- testing and testing methods if appropriate
- documentation of the change
- notifications to personnel or training as needed regarding the change
- Emergency MOCs
- Temporary MOCs

Alarm System Auditing

The PHMSA regulations and ISA-18.2 specify the alarm management system needs periodic auditing. API-1167 has a section on this as well, which is designed to satisfy the regulation.

An annual audit is about the work processes going into the overall alarm management program, not just the performance numbers.

Recommended contents of an annual audit include:

- verification that alarms are used only to represent situations requiring controller action to avoid defined consequences
- documentation of alarm settings and rationalization
- alarm documentation in the Master Alarm Database is current and sufficient to provide for proper controller guidance
- modification of alarms is properly controlled by MOC
- periodic alarm performance monitoring reports
- documentation of repairs to malfunctioning alarms
- documentation for out-of-service alarms
- roles and responsibilities for the alarm system users and support personnel are clear, documented, and known by appropriate personnel

Personnel interviews or questionnaires should be conducted as part of the audit to identify performance and usability issues. Interview topics may include:

- alarms occur only on events requiring controller action
- alarm priority is consistently applied and meaningful
- alarms occur in time for effective action to be taken
- roles and responsibilities for the alarm system users and support personnel are clear
- training regarding the proper use and functioning of the alarm system is effective

Action plans must be developed for problems identified during the audit process. When defining an action plan, timelines, accountabilities, and review of results obtained shall be assigned to each item.

Appendices

API-1167 has several useful appendices. These include:

- an example of a comprehensive Alarm Philosophy Document Table of Contents
- details of a widely used method for consistent and appropriate determination of alarm priority
- a summary of Alarm System Key Performance Indicators (KPIs)

Summary:

API-1167 is an important document which will get significant attention from PHMSA. It lays out the major principles involved in proper alarm management, specifically for the pipeline industry.

.

192/195 Regulatory Requirements. Alarm system-specific, partial, or related requirements are highlighted		
Alarm System Requirement	**Regulatory Section (192 = is Gas, 195 is Liquid)**	**Source of information to document compliance**
Have written control room management procedures	192.631 (a) 195.446 (a)	
Define several controller roles and	192.631 (b1, b2, b3)	

responsibilities	195.446 (b1, b2, b3)	
Record shift change/handover and document requirements for information exchange	192.631 (b4) 195.446 (b4) 192.631 (c5)	Status of controller-adjustable alarms and of alarm suppression should be covered
Provide adequate information to controllers by implementing certain sections of API-RP-1165	192.631 (c1) 195.446 (c1)	
Provide adequate information to controllers by implementing certain sections of API-RP-1168	195.446 (c8)	
Conduct point to point SCADA check when system is revised	192.631 (c2) 195.446 (c2)	Management of change documentation
Annually verify communication plan for manual pipeline operation	192.631 (c3) 195.446 (c3)	Recommendation: Cover as an additional non-alarm-related task in the annual audit
Test backup SCADA systems annually	192.631 (c4) 195.446 (c4)	
Implement several fatigue mitigation measures	192.631 (d) 195.446 (d)	
Have an Alarm Management Plan	192.631 (e) 195.446 (e)	The Alarm Philosophy Document, The Alarm Rationalization Plan and Schedule, and Annual Audit Reports
Review SCADA safety-related alarm operations	192.631 (e1) 195.446 (e1)	Alarm Rationalization
Monthly identification of several aspects of safety-related alarms and other performance monitoring	192.631 (e2,3,4,5,6) 195.446 (e2,3,4,5,6)	Monthly alarm analyses and reports, response documentation, Annual audit
Management of change, non-alarm-related	192.631 (f) 195.446 (f and f2)	
Implement section 7 of API-RP-1168 regarding control room management change	195.446 (f1)	
Operating experience: Incident review	192.631 (g1, g2) 195.446 (g1, g2)	Recommendation: Cover as an additional non-alarm-related task in the annual audit
Training – several requirements	192.631 (h1,2,3,4,5) 195.446 (h1,2,3,4,5)	Note: Alarm documentation provided in rationalization is one aspect of training
Documentation of compliance	192.631 (i) 195.446 (i)	

Figure 1: PHMSA Regulation Summary

The Seven Steps for Effective Alarm Management

Here is a brief outline of a best practices approach for a typical alarm management project. This methodology is proven through hundreds of successful projects. The first three steps are universally needed for the improvement of an alarm system. They are often done simultaneously at the start of a project.

Step 1: Develop, Adopt, and Maintain an Alarm Philosophy
Step 2: Collect Data and Benchmark Your Systems
Step 3: Perform Bad Actor Alarm Resolution

These first three steps are collectively provide the most improvement for the least expenditure of effort. They provide the best possible start and the fundamental underpinnings for the remainder of the steps necessary for effective alarm management.

Step 4: Perform Alarm Documentation and Rationalization (D&R)
Step 5: Implement Alarm Audit and Enforcement Technology
Step 6: Implement Real-time Alarm Management
Step 7: Control and Maintain Your Improved System

Step 1: Develop, Adopt, and Maintain an Alarm Philosophy

An Alarm Philosophy is a comprehensive guideline for the development, implementation, and modification of alarms.

Step 2: Collect Data and Benchmark Your Systems

Analysis is fundamental to improvement. You must analyze your alarm system to improve it. You should look for alarm analysis software with full graphical and tabular output, easy access to the full control system event journal entries, automatic report generation, and web-based report viewing. You want a comprehensive and complete set of alarm analyses to enable you to pinpoint your exact problems and apply the most efficient solutions.

Step 3: Perform Bad Actor Alarm Resolution

(To be covered in detail later in this paper.)

Step 4: Perform Alarm Documentation and Rationalization (D&R)

Many existing systems need a total rework, which includes a review of the configuration and purpose of every alarm. This is Alarm Documentation and Rationalization (D&R). The primary purpose is to ensure your alarm system is in alignment with your alarm philosophy. D&R can take quite a bit of effort, advice on performing it efficiently is recommended.

Step 5: Implement Alarm Audit and Enforcement Technology

Once your alarm system is improved, it is essential to ensure the configuration does not change over time unless the changes are specifically authorized. DCS and SCADA systems are notoriously easy to change, which is why software mechanisms that frequently audit (and enforce) the current configuration versus the Master Alarm Database are needed. Paper-based Management of Change solutions for DCS configuration (alarm or otherwise) have a wide and consistent history of failure.

Step 6: Implement Real Time Alarm Management

Based on the performance you need your alarm system to achieve and the nature of your operation, you may want to implement more advanced alarm handling solutions. These include:

Alarm Shelving: A safe, secure way to temporarily disable a nuisance alarm until the underlying problem can be corrected. Most control systems have inadequate mechanisms to properly control temporary alarm suppression. Computerized lists of shelved alarms, with time limits, reminders, and auto-re-enabling are necessary. It must be impossible to temporarily suppress an alarm and then forget about it, which is a very common and dangerous occurrence throughout industry.

State-based Alarming and Alarm Flood Suppression: Algorithms detect when the operating state changes (such as startup, shutdown, different products, rates, feedstocks, etc.) and dynamically alter the alarm settings to conform to the proper settings for each state. State-based settings for inadvertent shutdown of a piece of equipment have proven to be effective in managing most alarm flood situations.

Controller Alert Systems: Once the alarm system has been properly reserved for things meeting the requirements of what should actually be an alarm, there may remain a need for a controller-configurable notification tool explicitly separate from the alarm system. Such controller alert systems are a best practice and are described in API-1167.

Step 7: Control and Maintain Your Improved System

Operations and sensors change over time, and alarm behavior will change with them. Alarms working correctly now may become nuisances or malfunction in the future. Effective management of change methodologies, and an ongoing program of system analysis and correction of problems as they occur, is needed for an effective alarm system.

Details of Step 3: Alarm "Bad Actor" Resolution

Several categories of common problem alarms exist. Such alarms are often called nuisance or bad actor alarms. With enough bad actors, an alarm system is rendered virtually useless for the controller. This may lead to hazardous conditions, since important or critical alarms are lost in the sea of bad actor alarms.

Three primary tools will be used to correct the most prevalent bad actor alarms. They are:

- Proper alarm deadband configuration
- Proper process value filter configuration (with warnings!)
- Proper alarm delay time (on-delay or off-delay) configuration

You may be familiar with the first two, but not the third. Delay time analysis and adjustment is one of the most powerful techniques in existence for dealing with certain types of nuisance alarms.

Expected Results from Bad Actor Resolution

The top twenty most frequent alarms usually comprise anywhere from 25% to 95% of the entire system load. Obviously, if those alarms are dealt with successfully, then major system improvement will occur and with comparatively little effort. It is quite amazing that such high numbers of bad actor alarms exist, because it is doubtful that a highly skilled control engineer could actually design alarms to behave in the

ways we will discuss. Yet they do exist; all varieties are in almost every system we analyze.

The techniques in this section can yield very significant results. Here are some examples from fifteen different control systems:

Bad Actor Alarm Work Process Results	Baseline Alarms	Reduction from Bad Actor Recommendations	% Reduction
System 1	339,521	325,423	95.8%
System 2	644,487	593,904	92.2%
System 3	79,434	72,935	91.8%
System 4	58,049	51,782	89.2%
System 5	482,375	413,094	85.6%
System 6	414,887	333,395	80.4%
System 7	93,848	71,372	76.1%
System 8	64,695	46,749	72.3%
System 9	33,115	22,646	68.4%
System 10	225,668	133,307	59.1%
System 11	44,527	24,882	55.9%
System 12	183,312	77,417	42.2%
System 13	106,212	38,566	36.3%
System 14	91,686	29,188	31.8%
System 15	39,305	8,625	21.9%

Figure 2: Improvement Amounts from Alarm Bad Actor Resolution

In the above systems (See Figure 2), less than fifty alarms each were analyzed by the techniques in this section. The average percent reduction achieved was 66% (based on systems) or 77% (based on total alarms). This is a substantial gain for a small amount of work!

By doing this task near the start of an improvement effort, you immediately achieve a significant improvement and establish the credibility of the effort. You will be fixing things your controllers have probably known about for years, and may have just given up on ever getting fixed.

Chattering and Fleeting Alarms

Imagine an alarm which cycles between annunciating and clearing three or more times per minute. This is the definition we will use for a chattering alarm. Obviously, the clearing of the alarm condition is not due to a controller's detecting it, analyzing the situation, and making a change in the operation which then moves the process value and thus results in the alarm clearing. In fact, if you asked your best control engineer to design you an alarm to cycle in and out twenty or thirty times per minute, they would probably be at a loss as to how to do that. Yet, such chattering alarms are quite common. They are a big nuisance and distraction to the controller, but they are relatively easy to fix.

Both analog values and digital (on-off) signals, such as those from switches, can and do chatter. Digital values typically are the worst case.

There is a sub-category of alarms similar to chattering, called fleeting. These are alarms that come in and clear very quickly (too quickly for the controller to have been responsible), but do not necessarily repeat. The methods for addressing chattering alarms will also deal with these.

For chattering analog sensors, the first thing to consider is the deadband of the alarm.

Alarm Deadband

Alarms on analog values should have a non-zero deadband specified. As an analog value passes through an alarm setpoint, any noise or slight variation of the signal will cause multiple alarms if there is too small of an alarm deadband. And all signals have noise.

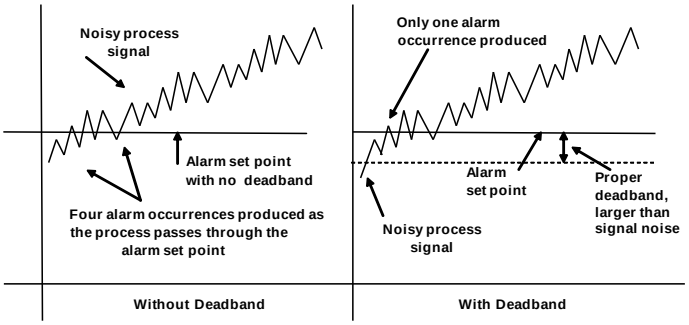

Figure 3: Deadband and Alarms

Figure 3 shows how a proper deadband, larger than the noise in the signal, reduces alarm events as the value moves above a high alarm setpoint. The alarm deadband should be specified to be larger than any expected signal noise. Most SCADA systems allow for deadband, but may specify it in measurement units, percent of range, or in some other way. The deadband's plus or minus positioning relative to the setpoint may also vary based on the alarm type. There may be individual deadband settings for each different alarm, or one applying to all of the analog alarms on the point. You have to check the SCADA documentation to configure deadband properly.

Deadband should be configured on every analog alarm. Rigorous calculation is not usually necessary; the following good starting values can be used.

SIGNAL TYPE	Deadband
Flow	5%
Level	5%
Pressure	2%
Temperature	1%

Figure 4: Deadband Settings Based on Sensor Type

Process Value Filtering and Alarms

It is possible to filter process variable signals in a SCADA system, usually in a variety of ways. The primary reason to use filters has to do with control loop performance. All signals have some noise. Noisy signals act to interfere with good control loop performance. An unfiltered noisy input signal to a PID (proportional-integral-derivative) controller will produce a noisy output signal. This will provide poor control and excessive valve movement and wear.

Control systems generally have a variety of filter algorithms to improve noisy variable signals. The use of filtering will have a similar effect on alarm activation, similar to deadband, and filters are mentioned here for that reason. An optimum filter setting is one that smoothes out signal noise, but has little effect on the desired response of the system. If a filter is too large, it may obscure operational problems from the controller.

Filters also introduce additional lag into control loops, which will be seen as additional apparent dead time in the loop. This may have a significant effect on the loop's settling time. A PID controller always has to be retuned after adding or modifying a filter on the variable.

The determination of proper filter settings for control is generally a full chapter in a control engineering textbook. It is more important for value filters to act correctly for control than for their resulting alarm effect. Therefore, we do not advocate signal filtering as a good way to address chattering analog alarms. They are mentioned here because they do have an alarm-related effect.

If you suspect you have a control problem related to a noisy signal, the following values are seen as good starting points for filters.

SIGNAL TYPE	Filter Time Constant
Flow	2 seconds
Level	2 seconds
Pressure	1 second
Temperature	-none-

Figure 5: Filter Time Constants Based on Sensor Type

Delay Time Analysis and Alarms

Deadband and process value filtering are applicable only to analog values. Often, the worst case chattering alarms or fleeting alarms are associated with on-off signals, such as pressure and level switches. While these devices may have a screwdriver-type, trial-and-error deadband adjustment on them (can you find the manual?), there is another powerful method to use; one that is probably already a capability of your SCADA system or can be added by a bit of logic or code. This method applies to both analog and digital point types.

The method and technique require a bit of explaining, but once explained, the technique itself is simple. The results you will get are so powerful it is well worth the effort.

There are two types of alarm delays available in many SCADA systems, namely the ON-delay and the OFF-delay. The OFF-delay is sometimes referred to as a "debounce timer." Some point or alarm types may have either delay available, and some only have one of them. Again, there is the need to read the SCADA documentation. These work differently and have significantly different implications when used. These settings provide powerful methods for dealing with chattering and fleeting alarms.

Since alarm analysis software is needed to improve an alarm system, let's make some use of it in not only detecting, but solving our problems. To do this, we want to take one of our nuisance chattering or fleeting alarms, and perform two frequency analyses on it. These are analyses of the time-in-alarm (duration) and time-between-alarms (interval).

Time-in-Alarm and Time-Between-Alarms

SCADA systems produce several time-stamped event records for alarms. Two of these are the alarm occurrence itself and the return-to-normal event, which is created when the condition causing the alarm to occur has cleared.

You will have recorded, in your alarm analysis software, thousands of occurrences from your nuisance alarms. For each specific nuisance alarm, take each pair of alarm occurrences and return-to-normal events, and then subtract the timestamps. The result is the time-in-alarm (duration) for the alarm occurrence. This can be done in a spreadsheet or database application.

In a similar method, subtracting an alarm occurrence timestamp from the prior alarm clear event timestamp produces the time-between-alarms (interval). Please see Figure 6.

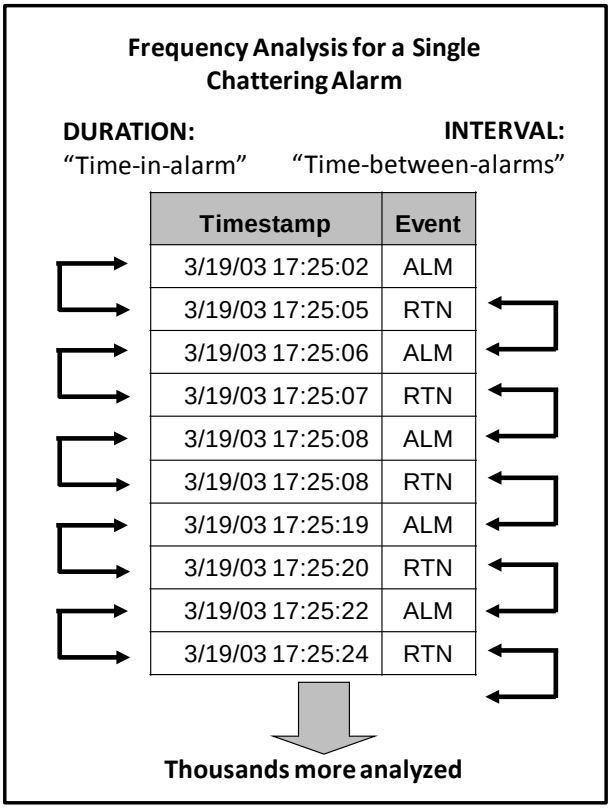

Figure 6: Chattering and Fleeting Alarm Durations and Intervals

Plot the results for thousands of events from a single alarm and you will often see a graph similar to Figure 7. In it, the two graph's curves are determined as follows:

- Time-in-Alarm (Duration) graph: Y = count of alarm occurrences having the DURATION of X seconds.
- Time-Between-Alarms (Interval) graph: Y = count of alarm occurrences having the INTERVAL of X seconds.

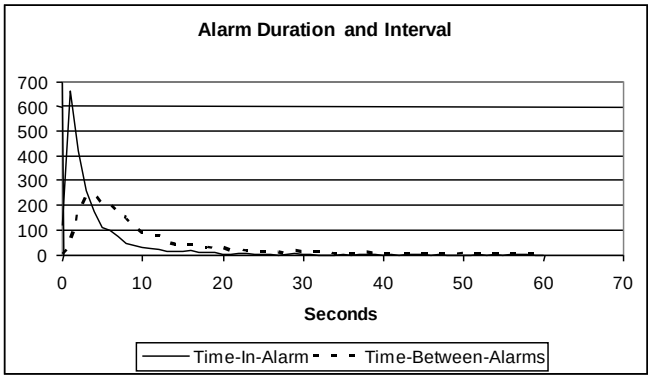

Figure 7: Alarm Delay Time Analysis Graph

In the case shown, based on thousands of alarm-return pairs, most of the alarms from this point have durations (solid line) less than ten seconds and the time-between-alarms (dotted line) is mostly less than twenty seconds. Obviously an alarm that comes in, lasts less than ten seconds, then goes away all by itself, does not meet the basic criteria for an alarm – something requiring controller action to resolve. When you plot these durations, the area under the curve totals 100% of the alarm occurrences from the single alarm being analyzed.

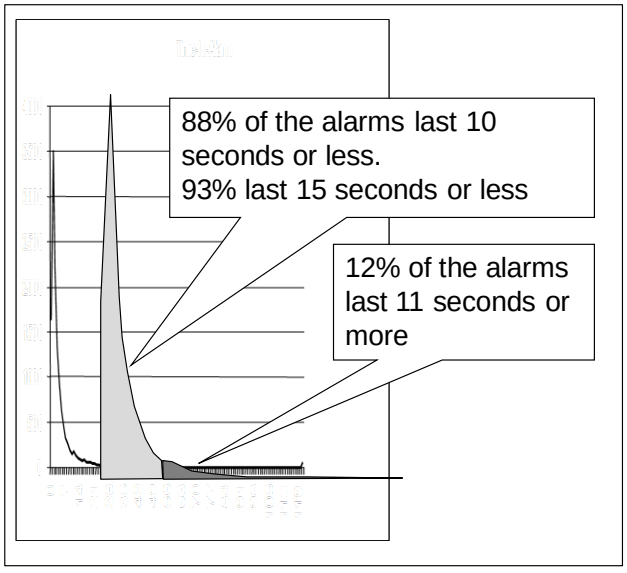

Figure 8: ON-Delay (Duration) Histogram Percentage Determination

In Figure 8, the alarm in question had thousands of activations lasting ten seconds or less. In fact, 93% of all activations of the alarm lasted fifteen seconds or less. Those alarms did not return to normal because of responsive controller action and thus indicated some sort of transient condition not requiring controller action to resolve. However some of the alarms did remain valid for several minutes.

This is very powerful information to use when coupled with the ON-delay and OFF-delay abilities of the SCADA system. Here is exactly how those abilities work.

ON-Delay

Use of the ON-delay time parameter can prevent a transient alarm from ever being seen by the controller. The alarm must remain in effect longer than the time specified before it is initially annunciated at all. The conversation goes like this:

NUISANCE ALARM TO CONTROL SYSTEM: Hey! I am in alarm!
CONTROL SYSTEM: Yeah, I get that a lot from you. I am going to wait – let's see – ten seconds before I tell the controller.
NUISANCE ALARM: 8 seconds later: Hey! I am not in alarm anymore!
CONTROL SYSTEM: Yeah, I figured that would happen. Good thing I didn't bother the controller with your prior message.

In this case, the alarm is only annunciated to the controller if the alarm lasts more than ten seconds without clearing.

The correct choosing of the ON-delay time parameter is quite important since, if used, even a valid alarm is not immediately presented to the controller. This will increase the overall time it takes for a proper response to be made. Such a delay could be a safety concern on some points. ON-delays of thirty seconds or less are generally not a problem for Priority 3 alarms. ON-delays of more than thirty seconds or a minute should be applied with much care, even for Priority 3 alarms. ON-delays of more than a few seconds are a concern for Priority 2 or Priority 1 alarms.

OFF-Delay

Use of this powerful method can turn a string of repetitive, nuisance, chattering alarms into a single, longer-duration alarm event. The OFF-delay timer must expire before a return-to-normal signal is processed and the alarm cleared. The conversation goes like this:

NUISANCE ALARM TO CONTROL SYSTEM: Hey! I am in alarm!
CONTROL SYSTEM: Right! I am telling the controller immediately!
NUISANCE ALARM, 11 seconds later: Hey! I am not in alarm anymore!
CONTROL SYSTEM: Yeah, I figured that would happen. Look, I am not going to tell the controller that you have cleared, because I think I know what you will tell me next. I am starting a 20 second timer on you.
NUISANCE ALARM, 18 seconds later: Hey! I am in alarm!
CONTROL SYSTEM: Hah! I was right! Good thing I didn't bother telling the controller that you had cleared. I will leave you in alarm.

In this case, the alarm is only shown as cleared to the controller when it has remained clear for more than twenty seconds. Using this technique, hundreds or thousands of nuisance repeating alarm occurrences can become a single, longer-duration alarm occurrence with no initial annunciation delay. The key is the correct choosing of the delay time parameter to be greater than the normal time-between-alarms.

The disadvantage to this technique also concerns the delay time. If the controller gets the alarm and takes a corrective action to eliminate it, he will not see a return-to-normal condition until after the delay time has expired, regardless as to if the action was immediately successful. In most cases, this is quite acceptable for OFF-delays of up to even a couple of minutes. Another concern is, for alarms chattering for long periods, the resulting "off-delayed" alarm may become stale, which is still a far preferable condition to chattering.(The source of the problem is probably that the alarm setpoint is too close to where the operation likes to live, and isn't really indicating a transition to an abnormal range.

Both on-delay and off-delay are applicable to both analog and discrete inputs (i.e., switches). Deadbands may be applicable only for analog signals, unless the discrete sensor has some sort of mechanical deadband adjustment.

For each alarm, it is straightforward to generate a table similar to Figure 9. This numerical analysis yields the exact percentage of how many alarms would be eliminated based on the choice and type of delay time. The table and charts let you see where the diminishing returns are, and to pick your delay correctly.

For this alarm, an ON-delay of thirty seconds would eliminate over 96% of the events. An OFF-delay of one minute would eliminate 72%. It is typical for OFF-delay to be less powerful than ON-delay; for the same specified time delay it will generally eliminate fewer alarm occurrences.

Delay in Seconds	% Reduction Time In Alarm (ON-Delay)	% Reduction Time Between Alarms (OFF-Delay)
5	77.7	19.7
10	87.6	37.8
15	93.0	48.7
20	95.4	58.4
25	96.1	62.4
30	***96.5***	64.1
35	97.6	66.5
40	97.8	68.7
45	97.9	69.6
50	98.2	70.6
55	98.5	71.6
60	98.5	**72.2**
65	98.6	72.4
70	98.7	73.2
75	98.7	73.6
80	98.7	74.1
85	98.7	74.6
90	98.9	75.1
95	99.0	75.7
100	99.0	75.8
105	99.0	76.0
110	99.2	76.4
115	99.2	76.9
120	99.2	77.2

Figure 9: Delay Time Alarm Reduction Table

Depending on the control system, there may be restrictions around the choices of delay types. These calculations are not determining why the chattering alarm behavior is occurring. The combination of the operating conditions and the sensing hardware results in chattering and fleeting behavior and a root cause investigation might find installation or hardware problems. The implementation of delay times is more of a highly effective band-aid solution.

The above table used actual occurrence data to determine the proper delay-time value. When implementing new points, you initially have no such data to use. What should be the defaults? This requires some explanation.

Implementation of either ON-delay or OFF-delay is different than the implementation of deadband. In specifying deadband, the physics

of the situation generally contraindicates the use of a zero default. But for many points, a zero ON or OFF delay may be perfectly acceptable.

Delays must be applied with care. Some important guidance is in Figure 10.

SIGNAL TYPE	ON Delay Time: Default is ZERO. Use ON-Delay only on identified problems and on Priority 3 alarms. Use on Priority 1 or 2 should be individually evaluated for acceptability.	OFF Delay Time: Default and use as shown for Priority 3 alarms. Use on Priority 1 or 2 should be individually evaluated for acceptability.
Flow	0-15 seconds	15 second default
Level	Use >30 seconds with care	30-60 second default. Use >30 with care, consider tank volume and throughput rates.
Pressure	Use >15 seconds with care	15 seconds default. Upper limit of 60-120 seconds is not usually a concern.
Temperature	Use >30 seconds with care	30-60 second default Upper limit of 60-120 seconds is not usually a concern.
Other	Individually consider. Often even a very short delay (5 seconds) will almost totally eliminate fleeting alarms.	5-30 seconds; use good engineering judgment based on the particular alarm.

Figure 10: Recommended Delay Times Based on Signal Type

Both of these methods are fixes or workarounds; they address the behavior of the alarm without determining the root cause as to why the signal is chattering or fleeting. Each type of input hardware, such as a switch may have different causes and compensation mechanisms. This technique does have the benefit of immediately addressing the chattering behavior, without suppressing the view of the alarm entirely from the controller, as alarm suppression would do.

While appropriate use of the methods can dramatically improve alarm performance, the underlying operational and mechanical causes should also be investigated This often involves review of sensors and installations. That is, of course, if you have the time, money, or people available to do that. Many places do not, and a great band-aid applied is sometimes a problem solved.

Stale (Long-Standing) Alarms

Stale alarms come in and remain in alarm for extended periods; more than twenty-four hours is a good starting value to use to identify them. They distract the controller by filling up the alarm summary screens. We have seen alarms that have been in effect continuously for years. (It is amazing what people will put up with.) They are often reflecting stable unit conditions, such as equipment shutdown or sensor malfunction, and generally indicate alarms that were not configured in accordance with proper principles, such as indicating only an abnormal condition.

Stale alarms can only be dealt with by an understanding of the operating states and hardware involved. They are usually eliminated by reconfiguring them so they truly reflect only abnormal, unexpected conditions requiring controller action to resolve. This may need some imagination, or implementation of some logic or state-based alarm methodologies.

Duplicate Alarms

Naturally, there are two types of duplicate alarms!

Dynamic Duplicate Alarms

Dynamic duplicate alarms are alarm occurrences consistently occurring within a short time period of other alarms. If you use your alarm analysis software to list the alarms always occurring within, for example, one second of each other, you will likely find a good list to work on. Such alarms are highly likely to be multiple annunciations, in different ways, of the same event. This is an undesirable situation.

The individual situation will determine which are kept and which are not, or what adjustments must be made. A high quantity of potential duplicates shows the need for rationalization to eliminate them.

Configured Duplicate Alarms

Interconnections between points in a SCADA system can create cases of duplicate alarm configuration. For example, a measurement may be sent from a sensor point to a selector point, to a totalizer point, to a logic point, to a controller point, and so forth. Often a bad measurement alarm is configured on each point, and thus if the sensor point goes into that condition, several simultaneous alarms will result. These distract the controller by annunciating multiple alarms caused from a single event. There should only be one such alarm, configured on the point where the controller is most likely to take the action. If a PID controller is involved, it (and not the sensor point) is the proper place, since the action to be taken from a bad reading is likely to put the PID controller in manual and adjust the output.

Nuisance Bad Measurement Alarms

It is quite surprising to see the amount of alarm occurrences on most systems that are from a bad measurement. These are often in the hundreds or thousands.

When the loop was designed, did someone tell the control engineer the following? “Oh, and by the way, I want this sensor to go into ‘Bad Measurement’ under the following (several) conditions and I want 650 ‘Bad Measurement’ alarms per week at a minimum.” And, if that had been told to the control engineer, could they have done it? Probably not! Yet, we find these on almost every system we look at.

Since no instrument was designed to be in such a state, every one of these situations can be fixed, and they should not be tolerated. They are misconfigured in range, in “measurement clamping”, or there is an installation problem (e.g., impulse leads filling up). The original justification for installing a flow meter probably did not include a specification that it was OK if it didn’t work half of the time! If that had been proposed, the money would have never been spent to buy it in the first place.

These situations must be addressed in a prompt manner since often an instrument malfunction removes an identified, rationalized indicator of an abnormal situation from the controller’s view. The time controllers spend confirming the instrument problem reduces their attention to other duties.

Generally, the addition of a new instrument must follow a MOC methodology to ensure it is done properly. The removal of an instrument does as well, to ensure it is truly not needed and the removal is done properly. And functionally, the indefinite toleration of a malfunctioning instrument is the same as removing it. If there is an incident, it will be difficult to explain how a relevant instrument was allowed to malfunction for months or to effectively be removed from service, without the appropriate level of review. This is the stuff of fines and lawsuits.

Long ago, the available instrument sensors had a significant tradeoff between accuracy (significant digits) and range; you could obtain high accuracy only over a small range, probably less than the possible variation of the measurement. Control engineers were well aware of this tradeoff and were accustomed to designing within those constraints. Then, along came the digital electronic revolution and these old constraints can usually be thrown out of the

window. Modern sensors can generally provide all of the accuracy needed over the entire range the measurement can experience. But some engineers continue to follow the older configuration practices and do not consider the consequences of generating lots of bad measurement alarms during conditions, such as startup and shutdown.

The default should now be to configure the instrument's range for the entire range of possible measured values (including ambient), and then see if the accuracy you get is enough. If not (rarely with modern transmitters), buy a better transmitter! However, don't configure the range where you know you will get a bad measurement state at ambient or shutdown conditions.

Differential pressure flows are often the worst offender. If, at zero flow, there is a slight imbalance in the leads, the meter attempts to report a slight backwards or negative flow. The flow range might not be configured for a slight negative, so the bad measurement condition and alarm occurs. Such points should be configured to handle the zero case. A cutoff can be configured and clamped at a zero value, so a small negative flow number is not actually used, which could affect some downstream calculations.

Most SCADA systems have the ability to clamp an analog value at the end of the range rather than go into a bad measurement state. This ability should be fully understood and used properly (i.e., read the documentation). Controller points using the value will usually have "shed modes." These are predetermined actions to take when a measurement goes bad and should be chosen with care.

Summary of Alarm Bad Actor Resolution Section

Nuisance alarms can be dealt with in several ways. Dealing with a very few alarms, in the ways shown, can create a large, low cost, and easily calculated improvement in an alarm system.

References

Hollifield, B. & Habibi, E. (2009). *The Alarm Management Handbook, Second Edition.*

Hollifield, B., Oliver, D., Habibi, E., & Nimmo, I. (2008). *The High Performance HMI Handbook.*

http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=INTERPRETATIONS&p_id=25164

http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=MOU&p_id=323

About the Author

Bill R. Hollifield, PAS Principal Alarm Management and HMI Consultant

Bill is the Principal Consultant responsible for the PAS work processes and intellectual property in the areas of both Alarm Management and High Performance HMI.

He is a member of the American Petroleum Institute's API RP-1167 Alarm Management Recommended Practice committee, the ISA SP-18 Alarm Management committee, the ISA SP101 HMI committee, and the Engineering Equipment and Materials Users Association (EEMUA) Industry Review Group.

Bill has multi-company, international experience in all aspects of Alarm Management

and HMI development. He has 26 years of experience in the petrochemical industry in engineering and operations, and an additional 9 years in alarm management and HMI software and services for the petrochemical, power generation, pipeline, and mining industries.

Bill is co-author of *The Alarm Management Handbook, The High Performance HMI Handbook,* and *The Electric Power Research Institute (EPRI) guideline on Alarm Management.*

Bill has authored several papers on Alarm Management and HMI, and is a regular presenter on such topics in such venues as API, ISA, and Electric Power symposiums. He has a BSME from Louisiana Tech University and an MBA from the University of Houston.