Smarter SCADA Alarming

Practical Ideas for Effective Alarm Management

Ignition!
by inductive automation

Practical Ideas for Effective Alarm Management

One day at about 4 p.m. in a waste water treatment facility located near your city, an alarm goes off when the water pressure gets too high in one of the tanks.

The alarm is set at priority level 4, which means "critical," but it doesn't stand out because almost all of the alarms at the facility are set at that level. Besides, the operator can't acknowledge the alarm right away because he's dealing with several other alarms that went off a few minutes earlier.

The operator hasn't yet realized that the earlier alarms were triggered by a pump that's turned off, as it's supposed to be at this state of the treatment process. A few minutes later, before he's gotten around to checking the alarm set off by the tank, yet another set of alarms goes off. The operator, who knows that almost all of the alarms in the facility prove to be "nuisance alarms" and who's tired near the end of a busier-than-usual workday, decides to silence all the alarms at once.

As a result, he remains unaware that the high water pressure in the tank is being caused by an input valve that was left partially open. Despite all of this alarm activity, a serious problem has gone unaddressed and it will only get worse as time goes on.

The scenario you've just read is fictional, but situations like it frequently occur in the real world, in all types of industries. Why are situations like these so common? Why is it that alarm systems so often mutate from a useful resource into a distraction that complicates problems more than it helps solve them? It's usually because changes are made to an alarm system over time without being carefully managed.

Organizations tend to set up an excessive amount of alarms and eventually lose sight of their purpose. Eventually, there are so many false or unnecessary alarms that the personnel often ignores them. The irony is that a flood of alarms can make the root problems harder to detect. If a serious problem is overlooked, it can result in losses of time, resources, money or, in the worst cases, life and limb.

Slowly but surely, the whole purpose of the alarm system will be defeated unless these types of changes are recognized and corrected.

A Poor Alarming System: A system with too many alarms can lead to alarm flooding, operator error and losses in time, money or worse.

800.266.7798
www.inductiveautomation.com

inductive automation
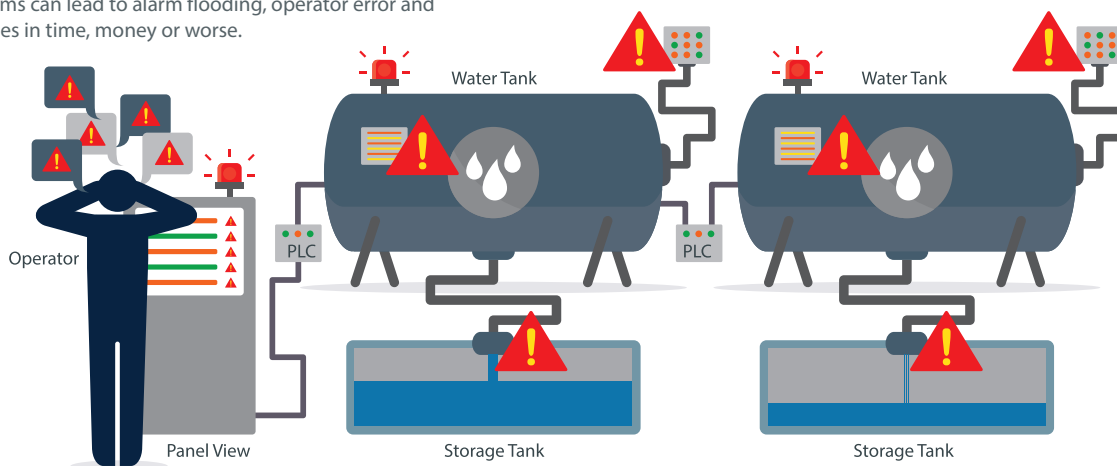
What's Wrong With My Alarm System?

To answer the question above, let's review some basics about alarms. There are three main events in the life cycle of an alarm: becoming active, becoming clear and being acknowledged. An alarm becomes active when the value it's attached to goes outside of its normal range, which is defined by high and low setpoints. An alarm becomes clear when a value returns to its normal range, at which point it drops out of the alarm system.

An alarm is acknowledged when the operator takes some action to indicate he or she is aware of it. The steps of clearing and acknowledging can vary in order. In the traditional concept of alarming, the system sends an alarm notification when an alarm goes active or is about to go active, often in the form of a one-way email to the operator.

Depending on the size of the operation, there are hundreds or even thousands of alarms that can potentially go off, and not all of them are valid. In every system, there will be unnecessary or meaningless alarms, which are sometimes referred to as "nuisance alarms" or "bad actors." Also, you'll often find "stale" or irrelevant alarms that stay in the alarm state continuously for over 24 hours, and "chattering alarms" that go from active to clear three or more times in one minute.

When there are too many alarms and they are not well prioritized, it often leads to a situation called alarm flooding in which an operator receives more than 10 alarms in 10 minutes. When operators are frequently inundated, alarm fatigue sets in. Operators may get into a habit of dismissing groups of alarms by clicking on "Acknowledge All" or even ignoring alarms sometimes.

Alarm problems can also arise because of poor work habits such as enabling all alarms by default, having inconsistent alarm practices between departments in the same company, and routinely using alarms to perform status checks rather than to bring attention to abnormal situations. These are all "alarming" practices in the wrong sense of the word, and they can result in missed alarms, operator error, production losses or worse.

How can you turn this situation around and get alarms under control again? The challenge of alarm management begins not so much with technology but with how you think about alarming. As you change your mindset about alarming, the technology side of the equation will become easier to sort out.

Rethinking Alarm Management

In 2006, *The Alarm Management Handbook: A Comprehensive Guide* by PAS principal alarm management and HMI consultant Bill Hollifield and PAS founder and CEO Eddie Habibi was published. It was soon republished by The International Society of Automation (ISA) under the title *Alarm Management: Seven Effective Methods for Optimum Performance*. It was well-received in the industry and a second edition was released in 2010. To many in the automation field, the principles in this book represent the standard for modern alarming practices.

The authors Hollifield and Habibi write, "In today's environment, proper configuration and management of your alarm system is not an option, it is a requirement. It is part of the cost of doing business." In the book, they propose steps for properly managing an alarm system: Develop, adopt and maintain an alarm philosophy; collect data and benchmark your systems; perform bad actor alarm resolution; perform alarm documentation and rationalization; implement alarm audit and enforcement technology; implement real-time alarm management; and control and maintain your improved system.

"In today's environment, proper configuration and management of your alarm system is not an option, it is a requirement. It is part of the cost of doing business."

— Bill Hollifield & Eddie Habibi
Authors of the *Alarm Management Handbook*

It is recommended that you read the book to determine whether and how to put its advice into practice at your company or organization. This white paper will very briefly summarize some of the book's main premises and ideas to give you a mental head-start on evaluating and rethinking your alarm system. It all begins with the first step the authors prescribe: developing and maintaining a new philosophy or mindset about alarming.

Philosophy: What is an Alarm?

Establishing an alarm philosophy starts with a look back at the basics. You should ask yourself: What exactly is an alarm, and which situations warrant using an alarm? Without answering this, you won't have an agreed-upon way of distinguishing false alarms from valid ones.

As basic as it seems, you should remember that an alarm should signal a real problem that requires some type of action by the operator. Alarms should always signify an abnormal event or condition; they should not be used to confirm that things are running normally. Alarms should never be ignored, and if they are being ignored you shouldn't try to solve the problem by adding more alarms.

If alarms aren't clear, if they aren't easy to understand and distinguish or if they occur more frequently than an operator can reasonably keep up with, they have ceased to be useful and have instead become the automation world's equivalent of "the boy who cried wolf."

If the last few sentences remind you of your alarm system, *The Alarm Management Handbook* advises that you thoroughly review everything related to alarming in your organization and create an alarm philosophy document. This document should serve as a comprehensive guideline for how alarms should be developed, implemented, prioritized, monitored, handled and modified. It should be the go-to document for every alarm topic and situation, even for team members who are unfamiliar with alarm management.

After you define your company's alarm philosophy, you should think about taking steps to prioritize and analyze alarms, implement real-time alarm management, review your alarm scheduling and notification

logic, and save and maintain the changes you make to the alarm system.

Prioritizing Your Alarms

Part of documenting your alarm philosophy involves reviewing how your alarms are prioritized. You should not have all of your alarms set at the same priority level because not all alarm situations are equally important, and because having too many high-priority alarms makes it more likely that operators will ignore them. To determine the proper priority for each alarm, you should combine two factors: how severe the consequences will be if no action is taken, and how much time is available for the operator to successfully respond to avoid those consequences.

The Alarm Management Handbook recommends using five priority levels: 0) Diagnostic, 1) Low, 2) Medium, 3) High and 4) Critical.

0	**Diagnostic**
1	**Low**
2	**Medium**
3	**High**
4	**CRITICAL**

Of those, only priority levels 1 through 3 should be used with any frequency while priority level 4 should only be used rarely, for true emergencies. Priority levels are meant to help the operator differentiate the importance of alarms. Because the most urgent alarms should stand out most, there should be fewer high-priority alarms than low-priority alarms. Use sound and color to differentiate alarm priority levels. When an alarm is acknowledged, its appearance should be altered in some way.

Analyzing Your Alarms

In order to improve your alarm system, you must analyze it. One of the first questions you need to

answer is "How many alarms does the system usually send out?" To establish a baseline, you should use at least eight weeks of continuous alarm data. You need to figure out how many alarms your operator can handle per day, and the maximum per day. It takes at least a few minutes for an operator to detect, identify, verify, acknowledge and assess an alarm, take corrective action and then monitor it. If your alarm rates are over 300 per day, they are simply too high. At that rate, operators have to ignore too many alarms. Two alarms in 10 minutes is the basic limit of what an operator can realistically manage.

You should also analyze how many alarms per 10-minute period to see how frequently alarm floods occur in your operation. *The Alarm Management Handbook* defines an alarm flood as when the rate of alarms exceeds 10 in 10 minutes. An alarm flood ends when the rate goes below five alarms in 10 minutes.

Also in *The Alarm Management Handbook*, the authors recommend using alarm analysis software with extensive graphical, journaling and reporting features. Furthermore, they write that you should analyze the bad actor alarms in your system and configure them to improve their performance. Usually, bad actors can be corrected by properly configuring the deadband (which is a range around the setpoint that a value must pass before setting off a discernible response), properly configuring the process filter or setting a proper delay time. Fixing chattering alarms is fairly straightforward once you commit to getting it done. By focusing on the most problematic alarms, you'll experience the greatest amount of improvement for your effort.

Using State-Based Alarming

Suppose that a production plant operates during the day and night, but it runs some of its machines only during the day. When those machines are turned off at night, their process values fall outside of their normal operating parameters. Should that cause an alarm to go off? Obviously not. To return to an earlier point, alarms should be used to indicate something unusual. If a machine is intentionally turned off, then its alarms should be disabled.

In the real-time alarm management technique called state-based alarming or alarm flood suppression,

alarm settings are dynamically adjusted to match the proper settings for each state. Before you implement state-based alarming, it's important to assess whether your process is a good candidate for it. It's a very effective practice for batch or semi-batch processes, and also good for processes that normally contain variables and different sets; for example, if your equipment works on different feed stocks or makes different products or grades, if your equipment has normal on-off modes during production, or if the off state normally results in differing sets of nuisance alarms.

Shelving Alarms

Imagine that one day at your facility, an important piece of equipment breaks down unexpectedly, interrupting production and triggering a number of alarms. You send your maintenance crew right away to fix the machine, but the alarms continue to sound. Since you're obviously aware of the problem, in this case, you temporarily silence the alarm while the crew works on fixing the problem. This technique is known as shelving an alarm.

Like state-based alarming, alarm shelving is a form of real-time alarm management. It is a temporary way to manually suppress alarms. Shelving is not intended as a long-term or indefinite solution for nuisance alarms. When done correctly, it's a good way to prevent alarm fatigue by setting nuisance alarms aside for a short time. After the alarms are shelved, the system continues to track their status and sends the operator a message about one

minute before the alarm shelf is set to expire so he can either un-shelf them or snooze them again. This prevents the operator from forgetting about the shelved alarms and keeps the system from just re-flooding him when the alarm shelf expires. Alarm shelving is somewhat like hitting the snooze button on a bedside alarm clock: you're temporarily shutting an alarm off but not canceling it completely.

Scheduling Alarms

If it doesn't make sense to enable alarms for a machine that's off, is it any more sensible to send an alarm to an employee who's off of work? By making sure your system is only notifying people who are currently on-shift, you'll reduce wasted alarms and avoid the mistake of notifying someone who cannot be expected to respond, let alone take any corrective action.

The key to accomplishing this is to have a reliable schedule of the people who get alarm notifications and when they should get them. In the traditional way of alarming, every user would receive notifications regardless of what time it was, or you'd organize different groups and give each group an expression to sort out which alarms it would get.

The new thinking in alarm scheduling is to provide workers with the ability to enter their schedule information so that an alarm that goes active at 9:01 a.m. will only go to the people working on the day shift, and an alarm that happens at 9:01 p.m. will only go to those working on the night shift. Or, when someone has a vacation coming up, they can enter that information in the schedule so they won't get notifications from the plant in Texas while they're working on their tan in Cabo San Lucas. Instead, the system will skip over the vacationing worker and immediately redirect the notification to someone who's available to help.

Having the flexibility to update schedules is not only convenient for employees but is more effective in getting a response when something goes wrong.

## Configuring Alarm Notification Logic

Who in your organization gets alarm notifications, and how often? How is the notification sent? This is mapped out in your alarm notification logic. By changing your alarm notification logic, you can take

greater control over what happens between when an alarm goes active and when the notification gets sent to its recipient. Below are a few different ways you can set up your notification logic.

Delay: One type of logic you could choose is a delay, which keeps the system from sending notifications until an operator who is close to the problem has had a set amount of time to deal with it. If the operator is able to fix the problem in time, that's one fewer notification that has to be sent.

Delay
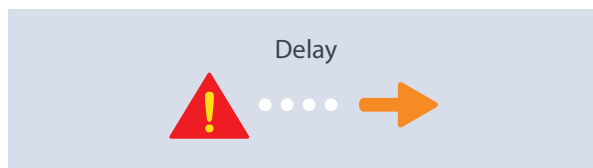
Escalation: Another type of logic is escalation, a term that is used for somewhat different alarming methods. To many people, escalation means something like this: The system sends a medium-priority alarm. If that alarm isn't acknowledged after a certain amount of time, its priority is increased to high and it is sent out again. However, escalation can also take other forms. You can start by showing the notification on the operator's screen and then, if necessary, sending emails five minutes later, and then making phone calls 10 minutes later. Or, you can prioritize contacts into groups and set up an alarm to go to a specified contact or group first, and then if that first contact or group doesn't acknowledge it, send it to a second contact or group. This form of escalation can often keep the task of responding to alarm notifications confined to a small group.

Escalation: Personal

Escalation: Groups

Consolidating: By consolidating multiple alarms into a single message, you can reduce alarm floods and the stress they cause. When a large number of notifications occur in a short time frame, you can send out one notification that tells the operator that there are 14 alarms to respond to instead of sending him 14 separate notifications. It feels more manageable to open a single message and step through a series of alarm notifications than to respond to several notifications occurring around the same time.

Consolidating
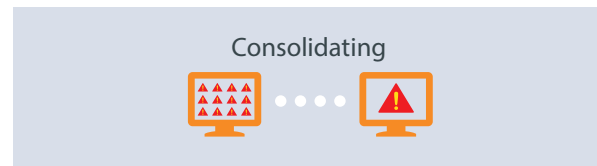
Choosing the alarm notification logic that best fits your process can alleviate many issues in your system.

Staying Connected With Your Alarms

In today's business world, you're expected to stay connected with what's going on at work even when you're not physically there. Why would alarm activity be an exception to this rule? You need to be able to monitor and manage alarming on-the-go, which means you need more than the usual one-way emails. As you think about your alarm system, consider adding two-way email, phone call, SMS notification or all three.

Two-Way Email: Email is a very convenient way to communicate that most of us use every day. When you have two-way email alarm notification capabilities set up, you can both receive and acknowledge alarm notifications by email.

Voice: The directness and urgency of a voice over the phone is a good way to get someone's attention. Voice alarm notifications reach contacts via a phone call and can be acknowledged with a simple key code, to the effect of "Reply with your PIN to acknowledge this alarm."

SMS: More commonly called text messaging, SMS has become widely used and it can be used as an efficient and immediate method for sending and acknowledging alarm notifications via mobile phones and devices.

Having more than one notification channel at your disposal not only keeps you better connected but also reduces the risk that a valid alarm gets overlooked or fails to reach the right recipients in time.

Saving Alarm System Changes

The Alarm Management Handbook recommends conducting a full review of the configuration and purpose of every alarm in your system. This methodology for determining, prioritizing and documenting alarms is referred to as alarm documentation and rationalization (D&R) or alarm objective analysis. Part of the D&R process is creating a master alarm database that contains proper setpoints, priorities, causes, consequences and corrective actions for each alarm.

Once you've made improvements to your alarm system, you need to ensure that any changes to the system configuration are not made lightly. You need to guard against making too many changes over time. It should be required that any properly handled alarm change also be updated in the master alarm database. The current configuration should be frequently audited against the master alarm database, preferably by good software.

An alarm philosophy document and a master alarm database will help you maintain the improvements you've made to the alarm system for a long time to come.

## Maintaining Your Improved Alarm System

Any system, no matter how well it's set up, will change over time. Those changes must be effectively managed, or your reconfigured system will regress into a suboptimal condition before long, and the time you've put into improving it will go to waste. It is essential to stay on top of changes to alarm priorities and setpoints, creation and deletion of alarms, changes of alarm type, changes of alarm descriptions or text messages, suppression of alarms, turning sensors on and off, changes in alarm graphics and changes to alarm handling capabilities. These system changes should be documented, communicated and approved just as any other change to your operational process would be. You should also audit your overall alarm management work processes at least annually.

As you rethink your alarm system and move forward with appropriate solutions, it's wise to keep this fundamental insight from *The Alarm Management Handbook* in mind: "Alarms are not a substitute for the constant surveillance of a qualified operator." As important as technology is to an alarm system, it will only be effective if the people behind it stay alert.

A New Standard in SCADA Alarming

When Inductive Automation developed the alarm features of Ignition, its SCADA and MES software, the development team had the principles from *The Alarm Management Handbook* firmly in mind. The application of these principles to the alarming needs of Ignition's global user community resulted in a fully integrated system that introduces new possibilities in SCADA alarming.
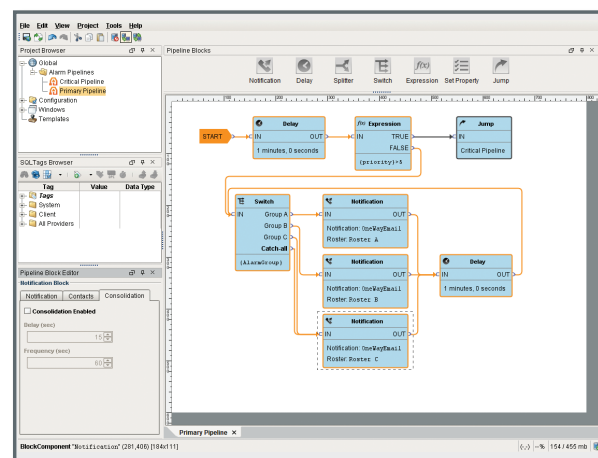
The Alarm Notification Pipeline in Ignition software allows for easy drag-and-drop alarm configuration.

Perhaps the most unique alarming feature in Ignition is its Alarm Notification Pipelines. This

"*Ignition has the power … to make your facility safer, more stable and more efficient.*"

innovative feature allows users to configure their alarm notification logic in a visual and intuitive way. Using a simple drag-and-drop interface, users can connect and loop together different kinds of pipeline blocks (Notification, Delay, Splitter, Switch, Expression, Set Property and Jump) to create many different configurations.

For example, users can set up where the alarm starts, then make it go into a five-minute delay block, then go into a Notification block to notify a specified group by email, and then make it jump into another pipeline. Or you could set up your pipeline so that high priority alarms are sent to Group A by voice notification over the phone and lower priority alarms are sent to Group B by email. With the Alarm Notification Pipelines, users can easily set up the escalation, delay, consolidation and selection logics mentioned earlier, as well as build their own unique logic.

Ignition software was built to support all of the alarming practices discussed in this white paper. Ignition allows users to easily suppress and prioritize alarms. It supports real-time alarm management, including state-based alarming and alarm shelving, and it records whenever those methods are used. It provides users with a wealth of alarm data from its powerful journaling system and associated data that adds contextual information to alarms. Two-way email, SMS and voice alarm notifications can all be added to Ignition through separate modules.

The Voice Notification Module is particularly unique because it can be tied in with a VoIP voice system or an online VoIP service such as Skype, it utilizes text-to-speech (TTS) technology instead of recorded sound files, and it supports alarm messages in a variety of languages. Ignition users can also bind multiple alarms per tag and bind alarm configuration properties to external data. Its call rosters make it easy to

organize users into groups, change schedules, assign roles and specify who should be notified at various points in the process.
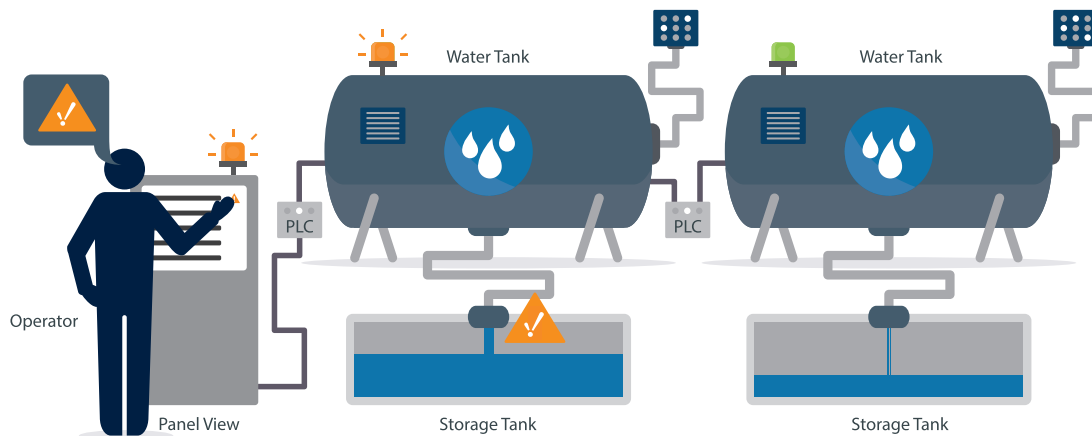
Ignition: Smarter SCADA Alarming

Ignition software solves many of the problems that develop in alarm systems. Let's revisit the fictional scenario from the beginning of this white paper and see how it would have gone better by using Ignition and applying some of the principles outlined here. When the alarm from the water tank came in at priority level 4, it would have gotten the operator's attention because most of the other alarms at the waste water treatment facility would have been set to a lower priority. The operator could have shelved the alarms that had gone off a few minutes earlier so he could focus on the priority-4 alarm. In Ignition, the alarm would have come with associated data from other units near the water tank, which would have helped him see that the input valve was causing the problem. When the earlier alarms were unshelved, he would have been reminded to handle them or snooze them a little while longer. By using Ignition the operator would have had fewer alarms to deal with and had more ways to manage them efficiently, so he'd be less likely to just ignore them. Most importantly, the root problem would have been identified and addressed before the situation turned more severe.

Ignition software has the power to make alarm management easier and more effective, from both a human and a technological standpoint, so that your company can put the best alarming practices into everyday use to make your facility safer, more stable and more efficient.

A Smarter Alarming System: With Ignition, alarms can be easily prioritized and managed so potential problems can be detected and solved quickly.