Keeping the peace (and quiet)

The solution is better plant-wide communication and understanding of the alarm philosophy.

By Roy Tanner, Jeff Gould, Rob Turner, and Tony Atkinson

Executing an alarm management strategy is no small task.

However, one of the hardest parts is sustaining the work done.

As plants change and expand, personnel turn over, and operations continue to remove obstacles in the way of production, nuisance alarms seem to creep back.

In order to continue your alarm management strategy and keep the peace, the challenges you will face range from getting various plant personnel involved to integrating the relevant systems.

Long, long ago alarm tales

You knew you had an alarm management problem for quite some time, and all of the signs were present. Operations managers would recommend using both sides of line printer paper as a cost-cutting measure because of the high number of alarms and events. In addition, as the control system caretaker, you noticed the number of operator keyboard and trackball failures that needed to return to service. After further investigation, you noticed during plant startups and shutdowns, the operators would repeatedly hit the acknowledge key until the annoying alarm tone would cease without calling up the alarm list. While this isn't true in all plants, it is probably true in most. You had it on your "to do" list to do something about this, but there was always some other project that was more visible with potential for more financially tangible results.

Finally, you had the go ahead to do something about this problem. Through years of increased focus on plant safety, alarm management was one of the more measurable means to tell how safe your facility actually was and therefore more visible. This, like many other trends, varies by region in degree to which regulatory agencies enforce such programs. For example, in the U.K., the Health and Safety Executive (HSE) has threatened prohibition notices where there is a lack of an alarm management program. In the U.S., organizations such as Occupational Safety & Health Administration (OSHA) are not yet as aggressive but are catching up fast. One reason for regulatory agency focus on alarm management is they can be more accurately monitored and regulated (as opposed to other safety related programs); another is over 42% of reported incidents have human error as a contributing factor.

These factors ranged from notification of alarm conditions, operators not knowing how to handle critical situations, and limited access to the proper operating procedures, to bypassed safety measures.

Compare analysis results
In order to execute your project, you probably read various articles in trade magazines and other sources, which gave you advice such as measure, analyze, and improve or benchmark, plan, and implement. While this made perfect sense, there were some details as to the how, which were not so clear. You forged ahead just the same and started with trying to assess how bad the problem actually was.

You tried to do some reporting through the control system and found out the reporting was not that easy; it was time-intensive and possibly did not cover all of the plant systems that need to be included.

So, you purchased a third-party alarm analysis software tool that collected the historical alarm and event data from the control system, as well as other plant systems, in place of a printer for future data collection. Though there was some tuning of how the analysis software treated the alarms, this was definitely less painful than manually moving, sorting, and writing queries against the data.

You compared your analysis results with the Engineering Equipment and Materials Users' Association (EEMUA) 191 guidelines, and your hand automatically slapped your forehead and slowly dropped down to your chin. This is a normal reaction when you find out the numbers are outrageously higher than the guidelines state.

The data collected clearly showed, at least in some plant states, the operators at your facility were operating in a reactive mode instead of predictive. Reactive is where operators have to react to certain conditions due to being flooded with alarms instead of using them to avert potential problems before they happen which is predictive.

After further analysis of the data took place, you developed a multi-faceted approach that converted your overloaded or reactive alarm annunciation status to more predictive.

- Reduce the number of nuisance alarms using analysis reports. The analysis tools pointed out some easy changes one could investigate and fix with little impact to operations. (Examples: chattering and duplicate alarms)
- Alarm rationalization and documentation: The size of this effort depends on the scope and the size of the facility. This is where a project happens to document tags, their configured alarms, and associated parameters to rationalize whether they are needed or not. Other data to be gathered is the cause, effect, and recommended action for the valid alarms. One should create an alarm philosophy document at this point, and it should act as the bible on the future handling of alarms at your facility.
- Dynamic alarm handling: During the analysis, it showed there were spikes of alarms during certain phases of production such as startups and shutdowns; therefore, some dynamic alarm handling would transpire in an attempt at reaching the desired EEMUA alarm statistics. This could be a large project if the alarm handling comes via logic running in a DCS controller or significantly smaller if the system has features to allow for more runtime alarm masking in the operator interface.

**Eureka! The job is over**

The quick hits to get rid of those nuisance alarm pests happened rapidly, and the operators seemed to appreciate it. The alarm rationalization project was more involved, and you acquired help from a vendor to help document and execute the information collected.

This took longer than expected, but well worth it, as now, you feel you're in control of your alarm configuration. Also, the task you thought would be more difficult, dynamic alarm handling, was actually
easier than expected due to new features in your latest control system that allow alarms to be dynamically hidden to the operator based on process conditions.

Although your results are not to the EEMUA recommendations, you can boast a 50% reduction during normal operations and close to 80% reduction in nuisance alarms during plant state transitions.

Months later, you decide to re-run some of the reports that you first ran for your benchmarking exercise, and it's lucky you did. Your once boastful numbers are not present any longer. How could this happen? ABB Engineering Services metrics indicate 97% of all new nuisance alarms come from one of three sources:

- Fault—usually it's the instrumentation
- Process change
- Minor project

After pondering this subject in your not-so-spare time, you develop a sound hypothesis for the return of the nuisance alarms.

Plant changes: In the time it took to complete some of the alarm reduction projects for your facility, other changes were taking place. There were projects for replacing older plant equipment as well as an expansion or two.

Of course, most of the changes that are giving you nuisance alarms aren't projects at all; they are a result of the inevitable drive towards efficiency and profitability from existing plant equipment. "Let's push that setpoint just a little higher" moves that noisy reading closer to the alarm threshold, or perhaps changing that controller tuning destabilized something else, causing an alarm downstream.

The problem was the people executing the DCS configuration work or moving those process variables were unaware of the ongoing alarm management efforts. While you are looking at the modifications, you notice all the new changes have implemented with the highest priority of alarm.

When you call the design engineer, he's emphatic that his project is of the highest importance and deserves the immediate attention of the operator in the event of a problem.

The solution to this is better plant-wide communication and understanding of the alarm philosophy created in earlier alarm rationalization efforts. This will ensure new projects and modifications follow this guideline and the work done to date will continue long after your promotion to another job.

Breakdown and equipment failure: Remember all those instrument faults you fixed when you did the original alarm reduction project? Guess what; they're back. Moreover, some of them are new.

You did remember to empower your maintenance guys to diagnose and fix faults that cause nuisance alarms, as well as create a procedure for shelving the alarms while they're undergoing repair, didn't you?

Change management procedures and reporting mechanism: In spot-checking some of the problem alarms you thought you corrected earlier, you find some of the alarm settings underwent some change as compared to the alarm rationalization documentation. You try to find a reason why, but it most likely happened soon after you changed them the first time. Putting these back in place is likely to take time, as you must get many approvals prior to making the required modifications. Perhaps you should have trained those process engineers while you were training the operations staff. Moreover, while you think
about it, maybe they should have a copy of the alarm design guide and alarm management philosophy you created.

**Best way to eat an elephant**

The one problem you can see from this exercise is that it seems like you're the only one that really cares.

Operations and maintenance personnel have enough to do already. Operations supervisors' main goals are to make production numbers, not for reducing nuisance alarms, and no one wants to be the scapegoat for not making quota.

The reality is everyone is doing some alarm management work today, but they are not doing it as efficiently as possible. Shift supervisors review inhibited alarms at the beginning of each shift. Operators scream to have nuisance alarms taken care of, but don't necessarily have the tools to say precisely which ones are causing the most grief. DCS technicians respond to the various requests from operations or maintenance and make the necessary changes, and finally maintenance desperately tries to squeeze in the requested instrument adjustments or equipment maintenance to address some of the issues. The problem is that for the most part, this is all gut feel.

What's necessary is a program that effectively deals with nuisance alarms without imposing bureaucracy and overhead. Experience shows the best team to deal with these alarms is the team already in place. You're not even required to be there (of course, you can stand by to claim the credit). Get this bit right, and soon the operations and maintenance people will realize getting on top of nuisance alarms makes their lives easier, not harder.

The trick is as simple as engraining very basic alarm review procedures into the existing work culture. By identifying the one or two alarm problems every week, and by simplifying the internal Management of Change (MOC) process to more seamlessly enable regularly required changes, your alarm system will be humming for years to come. The best way to eat an elephant is one bite at a time, right?

With things running smoothly, your operations team should be recognizing the problem early and be empowered and educated enough to determine the root cause and either fix it immediately or pass it on to the person who can resolve the problem. The maintenance team will already be dealing with those problems resulting from breakdown and will be aware of the nuisance alarm dimension. The engineers will be designing with alarm management in mind, and when they don't, they will get a prompt and focused push from the operations team. The operations supervisor will be periodically reviewing the status of alarms and the performance of the management system and making sure it is working smoothly. In addition, you will be in your office, taking all the credit. Maybe that leaves you enough time to look at the next level of operability; perhaps the EEMUA targets don't look that far away after all. Of course, the tools the team has to work with will make a big difference to the outcome.

**Software platform standards**

The solution is to get the entire facility involved with alarm management while not impeding production and minimizing the effort required. One way to do this is to streamline work processes through seamless integration of the various systems required to continue your alarm management strategy.

In the past, integrating a DCS with third party software was either a) impossible or b) expensive and hard to maintain. Similar to the realization that your car is a lemon because you know your auto...
mechanic on a first name basis, you know the solution was not a true integration when you totaled how much money went to maintenance at 'Joe's Software House' who implemented the solution. This situation was not always the integrator's fault, as the work went down from an end user specification, had limited infrastructure to work with, and was working with systems that didn't originate for the purpose of integrating into your system. In any event, there were dependencies on the integrators for modifications, routine maintenance, and upgrades.

Some of the latest automation systems use software platforms based on standards truly built for interconnectivity of applications and which take the management and communication of alarms fully into account. When these other applications are built to similar standards, such as ActiveX, OPC, HTML, XML, COM, Web interfaces, and others, the result is a better solution maintainable without being dependent on specific resources.

With this type of platform and use of standards, what needs seamless integration in order to streamline operations?

**Benchmarking/Analysis Tools:** The third-party software that was to collect and analyze alarm and event data is already collecting data automatically, but the pre-canned analysis reports were only available to the engineer on a separate computer. These reports should be readily available to the operations supervisor, maintenance technicians, and operators. If available with a mouse click, the right user can get access to the right report. Today's alarm analysis tools typically have Web-based report access for standard reports such as frequent, duplicate, standing, and chattering alarms as well as more general, performance statistic based reports to give the overall picture. The result is where an operations supervisor has access to alarm performance statistics or an operator can verify that a certain tag has nuisance alarms without going out of his or her normal work routine. Barriers such as special procedures, dedicated PC access, training, different passwords, forms, are non-existent.

**Asset Optimization:** Traditional asset management packages usually dealt with smart assets. Smart assets, such as HART, FF, or Profibus transmitters, have status information that aid more efficient preventative and predictive maintenance strategies. Today, asset optimization is now reaching beyond traditional asset management tools by monitoring devices that are simple network management protocol (SNMP) capable for computer and networking equipment status. Other assets are vibration detection sensors, analyzers, electrical devices such as drives and motor controllers, plant equipment such as heat exchangers, plant entities such as reactors, and even user defined data such as key performance indicators (KPIs).

By monitoring KPI information, the right people can be aware of status information that means more to the business objectives and notifies people in various ways that action is necessary. The use of Alarm Management performance statistics that yield information such as standing alarms, alarms per time period, and benchmarked information (such as whether areas of the plant are being operated in a reactive, stable or predictive mode,) can preemptively warn supervisors of possible problems. If caught early, these usually hidden problems can improve performance, reduce equipment wear and tear, and even prevent accidents.

**Notification Tools:** While asset optimization tools are great at monitoring and reporting issues, if no one ever looks at them, is there a problem that needs fixing?

You must have a notification methodology to alert the right people of issues that may arise from alarm management performance indicators and other monitored assets. One way is to have alerts come up to an operator screen, but this requires careful handling, otherwise they too become nuisance alarms. In
some cases, this can take place in a non-intrusive way that does not divert the operator's attention away from their responsible process area(s). Other means of notification are via e-mail, text messaging, and paging. Short message service (SMS) capabilities are automatically available in automation systems so when the number of standing alarms crosses a pre-defined limit or benchmark, the operations supervisor receives a page and concurrently the area engineer and plant manager get e-mails. While current supervisors, engineers, and managers are cringing at the idea of receiving yet another e-mail, it is likely their peers now facing criminal charges of negligence for not being aware of plant conditions during life taking/environment damaging incidents would welcome such an inconvenience.

**Computerized Maintenance Management Systems:** When integrating systems that result in the notification of potential problems, it makes sense to streamline the back end. In some cases, filling out a paper work ticket to fix these problems may be as intrusive as nuisance alarms. Many facilities use a computerized maintenance management system for tracking field assets such as transmitters, motors, pumps, and valves. Process automation alarm-management configuration should not be an exception. If nuisance alarms and/or alarm statistics sound off, the front line of defense, your operators or operations supervisors should be able to create a work order immediately, saving time and increasing the speed of resolution.

**Alarm Rationalization Data, Operating Procedures:** During the alarm-management-strategy execution, process-control tag data was collected and archived in order to improve the integrity of plant alarms. This data included tag descriptions, locations, tuning parameters, alarm configuration parameters, the alarm's probable cause, effect, and recommended action information. This data could be a valuable resource to operations during critical conditions; it should be operator assistance information, and it should be immediately available. In addition, links to current, up-to-date procedures can also help in the decision making process. Most incident reports indicated operations personnel didn't know how to react to certain plant conditions or lacked access to proper procedure documentation.

**Change Management:** During the alarm rationalization steps taken, the database contains key parameter information. In some cases, this database has features and reporting that enable it to work for change management purposes. For example, using this data to compare against current automation system settings could provide a difference report that indicates that values have changed. Audit trails and reports from both the change management database/system and the automation system can really speed up decision making as to what values are set incorrectly, who set them, and why. This information, if accurate and available quickly, can help avert costly mistakes and incidents that could potentially result in harm to personnel and millions of dollars worth of damage and lost production.

While it is hard enough to execute continuous plant improvement strategies such as alarm management, it is even harder to sustain them. Various plant personnel and plant systems must mesh and integrate in order to streamline the necessary activities required to continue the effort. It is easy to pound in a nail if you have a hammer, and the same holds true with accomplishing your integration goals. Some automation systems utilize platforms based on standard technologies that can help ease the integration effort to provide the best in class, maintainable solutions. What the end user must do is make sure their automation system investments, whether new, replacements, or upgrades, provide the necessary infrastructure that reaches beyond the traditional control system. This is paramount when considering continuous improvement programs that involve the entire plant. A solid technical foundation, combined with clear communication with your plant team, will ensure your program's ongoing success.

**Behind the byline**

Roy Tanner (roy.tanner@us.abb.com) has an electrical engineering degree. He is a marketing manager
at ABB. Jeff Gould (jeff.gould@matrikon.com) is a member of the ISA RP18.2 alarm management committee. He is a vice president is at Matrikon. Rob Turner is a senior consultant for ABB Engineering Services in the U.K. He is a chartered engineer through the British Computer Society. Tony Atkinson is a senior consultant for ABB Engineering Services in the U.K. and 27 years experience in design and management of control systems.