Auditing the alarm management system

Where is the problem?

By Ram Viswanathan

Alarm management practices have been in place in the process industries for many decades. With the ongoing developments in the various international standards, such as ANSI/ISA-18.2-2009, and recommended practices such as American Petroleum Institute (API) RP 1167, alarm management has gained greater importance.

The alarm management process life cycle consists of the alarm philosophy, design and implementation, monitoring, managing change, assessment, and the audit for improvement that reflects the familiar continual improvement practices in industries. While alarm performance monitoring measures alarm performance, the periodic audit ensures adequate management and work practices.

The essence of continuous improvement as dictated by the Deming cycle is in the “plan, do, check, and act” (PDCA) processes. The alarm management specification in the process industries can be well aligned with the PDCA cycle, as referenced by the ISO 9000 quality management principles. The ISO 9001 family of standards provides guidance and tools for companies and organizations to meet customer requirements and to improve the quality of products and services, and the requirements of alarm management standards are no different (figure 1).

By following specific auditing guidelines as per ISA-TR18.2.5-2012 (technical report) and API RP 1167 Section 10, the efficiency and effectiveness of the established system can be reviewed and improved. This article discusses the importance of the audit and the stages when it can be conducted.

Alarm management evolution

From the initial days developing Engineering Equipment and Materials Users Association (EEMUA) guidelines to the development of the ANSI/ISA-18.2 standard, alarm management processes have had a kind of evolution. To improve the evolution cycle, audit and continuous improvement must be the current focus of activity.

User requirements generally guide the evolution of systems, and alarm management is no different. Although the standards have developed from guidelines for annunciation and sequences, the systems have developed from the distributed control system to a more futuristic approach to managing alarms (figure 2).

Some of the futuristic practical applications of alarm management include advanced mathematical approaches like the fault diagnosis method based on artificial immune systems and dynamic alarm management based on Bayesian estimation. The integration of the two creates mechanisms to dynamically alter the alarm parameters for managing an abnormal situation. The crystal ball for alarm management shows the predictable future of alarm management developing further in data analytics and predictive processing.

Alarm system and alarm system management

The alarm system is a collection of hardware and software that detects an alarm state, communicates that state to the
operator, records changes in the alarm state, and monitors the system. Process control systems have built-in alarm systems to perform most of these activities. Additionally, advanced alarm management software complements basic systems with reporting features, alarm management of change process, and intelligent alarming techniques. It is also an external repository for alarms.

But alarm system management is the processes and practices for determining, documenting, designing, operating, monitoring, and maintaining alarm systems. This is guided generally by standards such as ANSI/ISA-18.2, and practices and guidelines from API, NAMUR and others.

The implementation of systems and processes themselves is not sufficient to achieve the alarm objectives; they have to be supported by an effective audit process.

Why audit?
Alarm management is the commitment operating companies make to stakeholders that safety is a critical focus of the operation and that they have the necessary steps to ensure that the mismanagement of the alarms will not be the primary reason for any abnormal situation. The Abnormal Situation Management (ASM) Consortium estimates that operation practices lead to costs of 3–8 percent of plant capacity due to unexpected events, resulting in substantial losses in production across the process industries.

As a result, individual operating sites could define the alarm system benefit as a measure of:
- Reduction in the number of equipment safety incidents
- Reduction in production loss time from improved abnormal situation management

Proper implementation of the alarm system management process has the following direct benefits:
- Effective operator role in managing the process
- Consistent, predictable operator action during abnormal situations
- Systematic approach to resolving process problems from data analysis
- Consistent engineering of the solution through the alarm configuration

The key component of operator effectiveness in the process industries is managing alarms. Hence the implementation of any system or process should directly or indirectly influence the operator to derive total benefit.

Earlier articles referred to achieving alarm management as a journey and highlighted the path to take and the importance of establishing the journey map. Cogging an audit process ensures that the path is effective and efficient.

The audit results with the objective evidence of the total benefits should be shared with operators so that they gain confidence in and continue to use the system.

Importance of audit
Many organizations have implemented both alarm systems and alarm system management and have been practicing them for a few years. They do the performance monitoring activities with the installed alarm system to improve alarm rates, but the importance of auditing the established system has not yet been widely practiced.

In addition to the API RP 1167 guidelines, a technical report developed by the ISA18 committee, ISA-TR18.2.5-2012, specifically focuses on the audit requirements to ensure the established system is reviewed, practiced, and improved. A periodic audit of the management process is called for to maintain the integrity of the alarm system and alarm management work processes.

Recognize that the purpose of implementing alarm management is not just about achieving the key performance indicators (KPIs) called for in standards and best practices, but ensuring that the established system realizes the process benefits. The alarm system should be an enabler of consistent and safe operation rather than a burden on the operation with additional administrative processes. The audit results should thus highlight the achievements of the overall established alarm management practices, such as improvements in the response time in abnormal situations.

Alarm management practices as per standards and best practices have been treated as "recognized and generally accepted good engineering practices" in US Occupational Safety and Health Administration guidelines. Hence the absence of such practices could be seen as a shortcoming, particularly in hazardous chemicals and transporting material in pipelines, if an industry wants to improve the safe operation of plants and other entities.

Auditing alarm management practices also tells operating companies the status of a control system to ensure safe and reliable processes. The audit is done for compliance to international standards and best practices and internal procedures. Organizations use audit results to develop and improve the alarm system and the performance of the personnel working with the alarm system to meet the objectives of the alarm philosophy.

Audit approach
The audit approach should be both for compliance and improvement. The compliance component addresses the applicability of the developed procedures to the best practices. The improvement component focuses on the efficacy of the established processes to achieving the stated objective.

In general, the audit program could cover the following areas in alignment with the PDCA life cycle approach. A typical approach is given in the table (figure 3), but it could be tailored to the site.

<table>
<thead>
<tr>
<th>Plan</th>
<th>Align with international standards and other best practices in the industry.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• The Alarm Philosophy Document audit highlights the planning process so opportunities for improvement can be identified.</td>
</tr>
<tr>
<td>Do</td>
<td>Execute the various procedures and processes mentioned in the Alarm Philosophy Document.</td>
</tr>
<tr>
<td></td>
<td>• Do a sample audit for review and compliance to the processes.</td>
</tr>
<tr>
<td></td>
<td>• If the audit results show similar types of problems, an opportunity exists to revisit the procedure; for example, the management of change process may have to be changed if it is not practical to follow some of the recommendations.</td>
</tr>
<tr>
<td>Check</td>
<td>Measure the KPI for all the established processes along with actual alarm data.</td>
</tr>
<tr>
<td>Act</td>
<td>Do improvement activities.</td>
</tr>
<tr>
<td></td>
<td>• objective evidence on process improvements</td>
</tr>
<tr>
<td></td>
<td>• demonstrated capability in abnormal situation management</td>
</tr>
</tbody>
</table>

**Figure 3. Audit process following the PDCA life cycle**

**How to conduct the audit**
The holistic approach of the alarm system audit should cover the different aspects of the alarm management process. Some of the requirements are audited by a mere questionnaire to understand...
the knowledge, training, and acceptance of alarm management practices, but others require randomly selecting sample events to audit. In general, the audit covers these aspects:

- Commitment by management personnel
- Awareness conveyed to all affected personnel
- Compliance to established procedures and practices
  - Direct: achievement of alarm KPIs
  - Indirect: efficient management of abnormal situations, loss of production, etc.

**Compliance to international standards**

Recognized standards such as ANSI/ISA-18.2-2009—and the soon-to-be-published IEC 62682 that is based on ISA-18.2—continually evolve and are revised regularly to match industry requirements. Organizations adopting these standards are required to review their management practices to stay consistent with the standards. Auditing alarm management practices at a defined frequency ensures current processes are used. To ensure best practices, organizations need to evolve with the standards. Auditing practices confirm compliance to pertinent standards.

**Compliance to internal procedures**

Aligning alarm management standards with already established internal procedures is critical to the success of the alarm management program. Some internal procedures that might influence alarm management practices are engineering discipline, risk assessment, and management of change procedures. The personnel auditing alarm management practices should be aware of the existence of such procedures and their adequacy.

**Phases of audit**

The standards recommend the audit should be conducted with a 12–15 month frequency. It may not be possible to conduct a total audit at a specified frequency, however, but a specific staggered audit could be conducted at the following phases of the organization over a period of 15 months:

1. “Greenfield” and “brownfield” operations
2. Impact of expansion or additional projects in a brownfield operation
3. Audit based on incident and problem reporting.

Additionally, a focused audit may be carried out to address a specific alarm management process such as management of change, monitoring, and alarm rationalization, depending on the area of deficiency.

**Focus areas**

The audit process is expected to cover all aspects of alarm management, but depending on industry experience, specific areas discussed below may require particular attention.

The roles and responsibilities of the personnel achieving the objectives of the established system are multidepartmental. The Alarm Philosophy Document needs to be clearly aligned with the site’s general organization structure so the recommended practices are followed without restrictions (e.g., the focus of electrical and instrumentation in addressing field issues to the technical department and process engineering group who determine the alarm limits and the process control group executing the recommendations from the different groups). However, operators on the panel are generally responsible to the operations department, and hence it is logical to assume that they are critical for achieving process objectives.

The audit process needs to establish the commitment of the different personnel to delivering their requirements. A typical responsibility matrix (figure 4) is a good starting point to address the requirement.

**Engineering discipline**

The engineering personnel, either internal or external to the organization, have significant influence on the:

- Alarm configurations
- Alarm suppression methodology
- Alarm configurations used in specific control schemes

Although it is important to follow an alarm rationalization process for the project work executed, it may be possible for engineers to execute small projects without completing the established standards. A sampled audit of alarm engineering processes should focus on the quality of the configuration, consistency in the methodology, and awareness by the personnel executing the projects.

Note that some of the engineering documents for configuring alarms may not be adequate or may be open to interpretation by the personnel doing the work, thus the audit must focus on

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibility</th>
<th>Operator/operations department</th>
<th>Control engineer</th>
<th>E&amp;I maintenance</th>
<th>Technical department</th>
<th>Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up alarm philosophy document</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Basic and advanced alarm design</td>
<td>X X X X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provide support and training</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Handle alarms and take actions to address the condition</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Provide recommended operator actions and document the same</td>
<td>X X X X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conduct alarm rationalization exercise</td>
<td>X X X X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test alarms</td>
<td>X X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report on the performance</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Periodic assessment and audits</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Figure 4. A role and responsibility matrix
Alarm priority assignment

Alarm priority assignment is the basic requirement in engineering an alarm. One accepted practice is to align alarm priority assignment with the company’s safety risk matrix. The safety consequence/likelihood matrix, used for reporting safety incidents, is translated into a consequence/recommended priority matrix. These two matrices differ in their application. For incident reporting the matrix is used after the incident occurred, whereas the alarm priority matrix is used to identify the potential consequence of a missed alarm (figure 5). Therefore, before applying the safety risk matrix, due diligence needs to be done to understand the relevance for deciding the alarm priority matrix.

Auditing the actual alarm rationalization process highlights compliance to the priority matrix, and due diligence is needed to decide on any modifications proposed to the alarm configuration.

Management of change issues

Although the benefits of following and implementing a change management process cannot be understated, the process itself faces the following challenges when implemented across process industries:

- Alignment with company procedures
- Auditing the management of change process

The standard KPI as per ANSI/ISA-18.2 requires that the number of unauthorized changes to the control system be zero. It implies the organization has to set up a mechanism to control the change and to measure and monitor the change process. Reasons for noncompliance are to be investigated. Any requirement for changes to the internal process for improvement will not only improve the scores, but also increase control room personnel’s confidence and level of acceptance of the change process.

Large organizations have a mature and effective management of change (MoC) for engineering and other process operations. Generally, the approval mechanism of the engineering processes is rigorous. While the process and procedure could be valid for alarm management MoC, take care in following the approval authority to avoid undue delay to alarm change implementation.

Consequently, the MoC process for a normal operation, such as a temporary change to trip points, would be approved by either the operations or instrumentation and control personnel involved with the process.

Conclusion

Dedicated focus to the auditing process in industries is vital to the productive evolution of the alarm systems and standards. Auditing the established processes and systems and evidence of their applicability in routine process operations is invaluable for the operating plant. The objective of alarm systems needs to be related to the improvements in the safety, incident management, and other related process benefits. Management should convey the importance of the audit process to the operators by sharing the results with them and demonstrating the importance of the system and the benefits thereof. Additionally, observed deficiencies also need to be highlighted to the operators so that they understand the larger role alarm management plays in operating their facilities.