Implement an Effective Alarm Management Program

White Paper
exida
80 N. Main St.
Sellersville, PA
www.exida.com

July 2012

exida White Paper Library
http://www.exida.com/Resources/Whitepapers

Introduction

Alarms are used in chemical processing plants to draw the operator's attention to an abnormal condition that, if disregarded, could lead to poor product quality, unplanned downtime, damaged assets, personnel injury, or a catastrophic accident. When employed appropriately, alarms help the operator to safely run the process within normal operating conditions. They are one of the first layers of protection to prevent the escalation of a hazard into an accident (Figure 1).

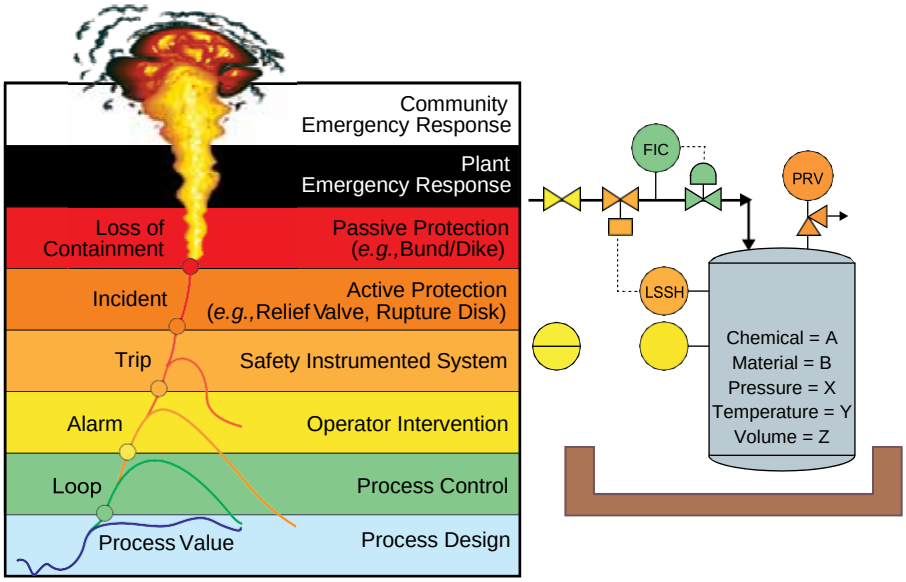

Figure 1: Alarms are one layer of protection to prevent the escalation of hazardous situations

Alarm management has become increasingly important as chemical plants look for ways to reduce costs, increase productivity, and deal with the loss of experienced operators. It has also become more challenging due to the adoption of the modern distributed control system (DCS). Alarm systems of the past consisted of panel- board control rooms, where the number of alarms was limited by the finite wall space, and there was an actual cost to hard-wire the system into the process (approximately $1,000 per alarm) *(1).* Today, alarms are considered free because they are implemented via software. Consequently, less thought goes into deciding which points should be alarmed and why. This has led to an epidemic of alarm management issues including:

- nuisance alarms (chattering alarms and standing/stale alarms)
- alarms identified with the incorrect priority level
- alarms that require no operator response
- alarms that occur frequently ("bad actors")
- alarm overload during normal conditions
- alarm floods during process upsets
- improper alarm suppression

Recognizing the increased importance of alarm management, the International Society for Automation (ISA) issued a new standard in 2009, ANSI/ISA-18.2, "Management of Alarm Systems for the Process

Industries" (*CEP*, Mar. 2011, p. 14). This article provides an overview of the standard and how it can be used to eliminate common alarm issues.

The Basics of the Standard

ISA-18.2 — developed by a committee composed of suppliers, consultants, government representatives, and end users of automation systems — provides a framework for the successful design, implementation, operation, and management of alarm systems *(2).* It contains guidance to help prevent and eliminate the most common alarm management problems, as well as a methodology for measuring, analyzing, and improving the performance of the alarm system.

The standard builds on a guide published by the Engineering Equipment and Materials Users Association (EEMUA), "Alarm Systems: A Guide to Design, Management and Procurement" *(3),* which was the primary reference for alarm management before the publication of ISA-18.2. The International Electrotechnical Commission (IEC) is using ISA-18.2 as the basis for an international alarm management standard (IEC-62682).

The ISA-18.2 standard takes a lifecycle approach to alarm management (Figure 2) that encompasses design, training, operation, maintenance, monitoring, and change management. Key activities are executed in the various stages of the lifecycle, and the products of one stage are the inputs for the next stage, as shown in Table 1.

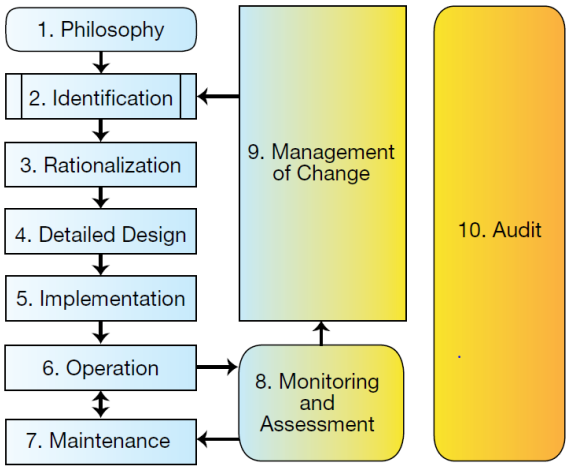

Figure 2: The alarm management lifecycle *(2)* consists of ten stages.

What is an Alarm?

The ISA-18.2 standard defines common terminology that can be used by all plant personnel when talking about alarms. Although this may seem rather insignificant, it is actually one of the most important accomplishments of the standard. An alarm is:

- *an audible and/or visible means of indicating* — for something to be considered an alarm, it must provide some sort of warning signal (a control device can be configured with limits that trigger control actions or data collection yet not be an alarm)

- *to the operator* — the indication must be directed toward the operator, not merely be a means to provide information to an engineer, maintenance technician, or manager

- *an equipment malfunction, process deviation, or abnormal condition* — the alarm must indicate a problem, not a normal process condition (such as an expected valve closure or pump stoppage)
- *requiring a response* — a specific operator response (other than acknowledging the alarm) to correct the abnormal condition and bring the process back to a safe and/or productive state must be necessary; if the operator does not need to respond, then the condition should not initiate an alarm.

Many alarm management issues are caused by alarms that do not meet these requirements.

Stage 1: Alarm Philosophy

The cornerstone of an effective alarm management pro- gram is the alarm philosophy document, which establishes guidelines for addressing all aspects of alarm management, including the criteria for determining what should be alarmed, roles and responsibilities, human machine interface (HMI) design, alarm prioritization, management of change (MOC), and key performance indicators (KPIs). This document is critical for helping plant staff maintain an alarm system over time and for driving consistency.

It is important to establish the methodology for alarm prioritization and classification before beginning alarm rationalization — *i.e.,* the process used to ensure that every alarm is valid and necessary. Priority is used to indicate how critical the alarm is and to help the operator know which alarms to respond to first. To ensure consistency, alarms should be prioritized based on the severity of the potential consequences and the time available for the operator to respond. Alarm classification organizes alarms based on com- mon characteristics and requirements (*e.g.*, testing, training, MOC, reporting). Certainly, an alarm that is identified as a safeguard in a hazard and operability (HAZOP) study or as an independent protection layer (IPL) will have more-stringent requirements for testing and operator training than the average process alarm. A good philosophy provides a listing of relevant alarm classes (*e.g.,* critical for personnel safety, quality, environmental protection, process safety, compliance with the U.S. Occupational Safety and Health Administration (OSHA) process safety management (PSM) standards), and their requirements. The philosophy stage also includes preparation of the alarm system requirements specification (ASRS), which identifies the alarm system's functional requirements. The ASRS can be used to support vendor selection, serve as the basis for system testing, and help in determining whether any advanced/enhanced alarming techniques, such as customization or third-party products, are needed.

Table 1. The alarm management lifecycle consists of ten stages that direct the design and implementation of an effective alarm system.		
Activity	**Inputs**	**Outputs**
Stage 1: Philosophy		
Document the objectives, guidelines, and work processes for the alarm system	Objectives and standards	Alarm philosophy document, alarm system requirement specification (ASRS)
Stage 2: Identification		
Determine potential alarms	Process hazard analysis (PHA) report, safety requirements specification (SRS), piping and instrumentation diagrams (P&IDs), operating procedures, etc.	List of potential alarms
Stage 3: Rationalization		
Determine which alarms are necessary, establish their design settings (*e.g.*, priority, setpoint, classification), and document their basis (cause, consequence, corrective action, time to respond, etc.) in a master alarm database	Alarm philosophy, and list of potential alarms	Master alarm database (MADB), alarm design requirements
Stage 4: Detailed Design		
Design the system to meet the requirements defined in rationalization and philosophy; includes basic alarm design, human-machine interface (HMI) design, and advanced alarming design	MADB, alarm design requirements	Completed alarm design
Stage 5: Implementation		
Put the alarm system into operation (installation and commissioning, initial testing, and initial training)	Completed alarm design and MADB	Operational alarms, alarm response procedures
Stage 6: Operation		
Alarm system is functional. Operators use available tools (*e.g.*, shelving and alarm response procedures) to diagnose and respond to alarms	Operational alarms, alarm response procedures	Alarm data
Stage 7: Maintenance		
Alarms are taken out of service for repair and replacement, and periodic testing	Alarm monitoring reports and alarm philosophy	Alarm data
Stage 8: Monitoring and Assessment		

Measure alarm system performance and compare to key performance indicators (KPIs) defined in the alarm philosophy; identify problem alarms (nuisance alarms, frequently occurring alarms, etc.)	Alarm data and alarm philosophy	Alarm monitoring reports, proposed changes
Stage 9: Management of Change		
Process to authorize additions, modifications, and deletions of alarms	Alarm philosophy, proposed changes	Authorized alarm changes
Stage 10: Audit		
Periodically evaluate alarm management processes (*e.g.*, comparing control system alarm settings to the MADB)	Standards, alarm philosophy, and audit protocol	Recommendations for improvement

Stage 2: Identification

Potential alarms are identified by reviewing plant and process documentation. This documentation includes process (or piping) and instrumentation diagrams (P&IDs), process hazard analyses (PHAs), operating procedures, product quality reviews, layer-of-protection analyses, safe operating limits, failure modes and effects analyses, environmental permits, and the existing control system configuration.

Candidate alarms should not be considered valid until they have successfully gone through the rationalization process (discussed next). Even alarms that have been identified as safeguards in a HAZOP analysis must be rationalized.

The criteria for determining whether an alarm is valid should be applied when the alarm is first identified (*e.g.*, during a hazard analysis) and its basis (*e.g.*, purpose, cause, potential consequence, and time to respond) should be documented. These forward-thinking activities will improve the quality and amount of information available for this evaluation.

Stage 3: Rationalization

The modern DCS makes it easy to add alarms without significant effort, cost, or justification. To avoid unnecessary alarms, alarm rationalization aims to identify the minimum set of alarms needed to keep the process safe and within its normal operating range, and to ensure that every alarm is valid and necessary. This is a multistep process that includes defining and documenting the design attributes (*e.g.*, priority, setpoint, type, and classification), as well as the cause, consequence, time to respond, and recommended operator response in a master alarm database (MADB). It is a team activity (similar to a HAZOP study) involving pro- duction and process engineers, process control engineers, experienced operators, and other personnel as needed.

Alarm validity. The first step in the rationalization process is to verify the validity of the alarm based on the criteria set forth in the philosophy document. If the candidate alarm does not meet the criteria — *e.g.,* it does not represent an abnormal situation, it is not unique, it does not require a timely operator response, etc. — it can be removed from consideration.

Consequences. Next, the consequences of inaction — that is, the direct and immediate consequences of failing to manage each individual alarm — are identified. This step is not concerned with what could happen if all protection layers fail — the ultimate consequence — as defined in a HAZOP. If inaction does not generate significant con- sequences, for example if the only consequence is the generation of another alarm, the alarm may not be needed.

Operator response. Another important step in identifying and eliminating unnecessary alarms is documenting the steps to be taken by the operator to correct the abnormal situation, such as closing a valve or starting a backup pump. If an operator response cannot be defined, then the alarm is not valid and can be removed from consideration. If multiple alarm conditions share the same opera- tor action, this may indicate redundant alarms, and one or more can be eliminated.

Response time. After determining how the operator should respond, the time available to take this action is estimated. Operator response time is defined as the time between the activation of the alarm and the last moment the operator can act to prevent the consequence; thus, it represents the time available to the operator to fix the problem. If the available time is insufficient, the alarm should be redesigned (because it will not be reliable) and replaced with an automated response (*i.e.,* an interlock).

Alarm priority. Alarm priority is established based on operator response time and severity of the consequences, which are assessed against predefined thresholds in areas such as safety, environmental impact, and cost. ISA-18.2 recommends a maximum of three or four different priori- ties. To help operators respond effectively to the most critical alarms, only a small fraction should be set to high priority (*e.g.,* 5%), with the remainder set to medium (15%) or low (80%) priority.

Alarm class. Alarm class is assigned based on the type of consequences and the method used to identify the hazard and consequences (*e.g.,* a HAZOP analysis). Alarms can be assigned to more than one classification.

Setpoints. Alarm setpoints (limits) should be defined far enough away from the consequence threshold to give the operator adequate time to respond, yet not so close to nor- mal operating conditions that nuisance alarms are triggered as a result of normal process variation. A common mistake is to configure setpoints based on rules of thumb relative to the range of a process variable. An example is configuring the setpoints for high-high, high, low, and low-low as 90%, 80%, 20%, and 10% of range, respectively.

Advanced alarm handling. Lastly, one should evaluate the need for advanced alarm handling by documenting states, conditions, steps, phases, or products for which the alarm limit or priority should be different from steady state, or the alarm should be suppressed from the operator. This helps to ensure that an alarm is always relevant when it is presented to the operator.

The results of this rationalization process are recorded in a master alarm database (MADB), which can range from a user-developed spreadsheet to a commercially available tool (Figure 3).


Alarm List - Operator Decision Support

LAHH103, LT103 *

Base Response On	Process Safety Time (minutes)	Cause	Confirmation
Consequence Of No Action	30	LV-201 fails closed causing loss of control in LIC201.	KO Drum Level - LIC201 KO Drum High High - LAH202
Liquid carryover to K-102, equipment damage, personnel exposure	Design Intent		
	Prevent KO Drum from overflowing		
Alarm Message		Corrective Actions	Comments
KO Drum High High Level	☑ Alarm Enabled	Manually open valve LV201	Alarm should trip SIS Interlock I-101
Priority Level	☑ Include in Alarm Response Manual		
Warning			

Figure 3: The rationalization stage identifies (among other things) the cause, consequence, and corrective action for each alarm, and records he information in the master alarm database. (Source: SILAlarm, exida 2012)

Stage 4: Detailed Alarm Design

Basic alarm design. In basic alarm design, alarms and alarm components are designed and configured based on the requirements identified in the rationalization stage. This includes the establishment of alarm deadbands and on/off delays, as well as basic logic to define when the alarm should be active. For example, in some plants, motors and pumps generate a nuisance alarm whenever they are not running, instead of alarming only when they stop unexpectedly. Nuisance alarms are defined as alarms that activate excessively, unnecessarily, or do not return to normal after the correct response is taken.

The alarm deadband compensates for fluctuations in the process variable, reducing the number of times an alarm triggers for a given abnormal condition, which should be only once. Deadband adds an offset to the alarm limits to prevent an alarm from returning to normal until the process variable clears the limit by this additional amount.

The deadband should be set wide enough to accommodate the expected noise level in the variable's measurement, but narrow enough to ensure that the alarm is meaningful. This will minimize chattering alarms (*i.e.*, alarms that repeatedly transition between the alarm state and the normal state in a short period of time). On/off delays can also prevent chattering alarms. Industry studies have demonstrated that following recommended practices for use of alarm deadbands and on/off delays (like those in ISA-18.2) can reduce the alarm load on the operator by up to 90% *(4).*

Human machine interface (HMI) design. An effective HMI design maximizes the operator's situation aware- ness, helping him or her see the big picture and proactively address process deviations before they become more serious. Graphic displays should provide an appropriate level of process and equipment information for the operator to verify or confirm the existence of an alarm. A well-designed HMI enhances the operator's ability to detect new alarms quickly, diagnose the cause of the problem, and respond with the appropriate corrective action.

HMI graphic displays should be designed so that alarms "jump off the page," drawing the operator's attention to the alarm rather than less-important information (*e.g.*, pump status). The level of visibility of information should be related to its operational importance — background information should have low visibility, normal plant measurements medium visibility, and abnormal conditions (values and states) the highest visibility.

The appropriate use of color, text, and patterns helps the operator detect the presence of an alarm and determine the order of priority. Certain colors should be reserved for alarms and not be used for other functions within the HMI (such as equipment status or process piping). Alarm colors should reflect the

priority of the alarm. In addition to color, symbols, patterns, and/or text should also be used to indicate alarm status, because approximately 8%–12% of the male population is color-blind.

Enhanced and advanced alarming. Overloading the operator with stale alarms (alarms that remain activated for an extended period of time, *e.g.,* more than 24 h) or alarm floods (10 or more alarms in 10 min) can lead to increased operator stress, missed alarms, and/or operator error. An effective alarm system manages the number of alarms presented to the operator and ensures that they are presented only when they are relevant and when they require a response. Transient plant conditions, the use of different feedstocks, production of different products, idled equipment, and unplanned process upsets can make this a challenge. In batch processes, for example, a large number of nuisance alarms result from not suppressing alarms during steps in which they are not applicable. The CSB investigation of the accident in Belle, WV, *(5)* found that the control system was not engineered to suppress nuisance alarms originating from idled process equipment.

In advanced alarming, additional layers of logic, programming, or modeling are used to modify alarm attributes such as setpoint, priority, or suppression status based on the state of the process and/or equipment. Alarm suppression — preventing the alarm from activating when the base alarm condition (*i.e.,* the condition that would normally generate the alarm) is present — is a common technique. ISA-18.2 defines three types of suppression (although the terminology and functionality vary among different control systems):

- designed (automatic) suppression — suppresses alarms based on operating conditions or plant states, for instance when equipment is out of service or in response to an event (e.g. a compressor trip) that would otherwise lead to an alarm flood; this is controlled by the logic that determines the relevance of the alarm
- shelving (manual) suppression — a mechanism, typically initiated by the operator, to temporarily suppress an alarm
- out of service — the state of an alarm during which the alarm indication is suppressed, typically manually, for reasons such as maintenance.

ISA-18.2 defines other types of advanced and enhanced alarming methods, including time-varying alarm attributes, redirection of alarms (*e.g.*, via pagers) to personnel outside the control room, and techniques for automatically deter- mining the cause of abnormal situations.

Advanced alarming could be applied, for example, to a reactor and its associated temperature, pressure, level, and flow alarms. When the reactor is in operation, alarm limits could be set differently depending on the product that is being made or the step of the batch recipe that is underway. When the reactor is idle or offline for maintenance, most of the alarms will not be useful and some might be triggered unnecessarily. Alarm suppression can hide these unnecessary alarms, which would otherwise remain active until the equipment is put back into service, thus becoming stale alarms.

Before suppressing an alarm, it is important to con- sider whether it is needed to detect a hazardous condition even when the process or equipment is out of service. The alarms for reactor high pressure and flow might be required to detect a leak (which would indicate a loss of isolation from the process). Thus, these alarms should not be sup- pressed and their limits should be set to detect the abnormal condition.

Stage 5: Implementation

The alarms are put into service in the implementation stage. This stage includes commissioning, training, and testing, all of which are ongoing activities that result from process design changes or the addition of new instrumentation.

For alarms to be effective, the operator must know how to respond to each alarm. An effective training program covers all realistic operational situations, including:

- system functionality and features such as sorting/filtering, navigation, and shelving
- principles of the process to ensure a full understanding of why the alarm is created as well as what could happen if the alarm is disregarded
- procedures that should be followed to shelve an alarm or take it out of service.

Training is particularly important for safety-related alarms, such as those identified as a safeguard, as an independent protection layer, or as part of an OSHA PSM mechanical integrity program. These alarms do not occur often — typically only in periods of high operator stress such as during a major plant upset.

Stage 6: Operation

During the operation stage, alarms perform their function of notifying the operator of an abnormal situation. A useful system provides tools, such as shelving and alarm- response procedures, to help the operator handle alarms.

Shelving is critical to responding effectively during a plant upset, as it allows the operator to manually hide less- important alarms on a temporary basis. In some systems, shelved alarms reappear automatically after a preset time period so that they are not forgotten.

The alarm philosophy should specify which alarms can be shelved and by whom, as well as which alarms cannot be shelved (*e.g.*, those that are of the highest priority or related to personnel safety). Systems that support shelving require that the operator be able to view a list of all shelved alarms for review anytime, such as during shift change.

A key best practice is providing operators with alarm- response procedures. Alarm-response procedures contain process knowledge that was captured during rationalization (*e.g.*, cause, consequence, corrective action, and time to respond), typically based on input from senior opera- tors. This information, provided in context to the operator from within the HMI (Figure 4), can be indispensable for helping operators (especially junior operators) respond to alarms more quickly and consistently.

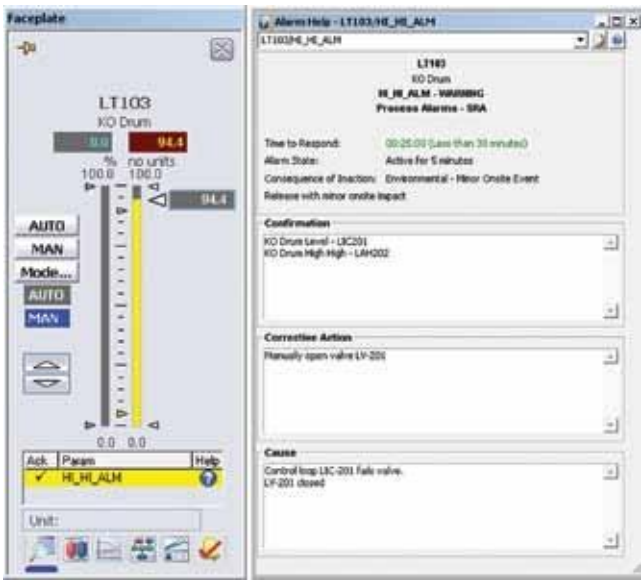

Figure 4: The alarm-response procedure can be integrated into the HMI to give operators easy access to critical information. (Image courtesy of Emerson Process Management)

Stage 7: Maintenance

The maintenance stage is concerned with alarms that are out of service, typically for equipment repair, replacement, or testing. The out-of-service state is not a function of the process equipment, but describes an administrative process of suppressing (*i.e.*, bypassing) an alarm using a permit system.

The ISA-18.2 standard provides recommendations on what should be contained in a procedure to remove an alarm from, and return it into, service. Recommendations include documenting why an alarm was removed from service, assessing the impact on safety, and defining what testing is required before putting an alarm back into service. Prompt repair of hardware failures is important to minimize alarms associated with the failures, as these alarms can quickly become stale or nuisance alarms that interfere with the operator's ability to detect new alarms. If prolonged out-of-service periods are required, then interim alarms may be necessary.

Periodic testing of alarms is an important maintenance activity for verifying alarm integrity. The frequency of testing is typically dictated by the alarm's classification and expected frequency of activation. For example, IPL alarms should be proof tested at a rate based on their expected level of risk reduction, whereas alarms that are part of an OSHA PSM mechanical integrity (MI) program should be tested according to the MI program's requirements. One of the findings of the Buncefield investigation of the fire and explosion at the Hertfordshire oil storage terminal in Hertfordshire, England *(6),* was that the design and location of the failed independent high-level safety switch made it difficult to test, and its integrity could not be verified.

Stage 8: Monitoring and Assessment

During the monitoring and assessment stage, plant personnel measure the performance of the alarm system and compare it to the KPIs identified in the philosophy document. Results are analyzed to identify issues such as nuisance alarms, bad actors, and alarm overload. All of these can clutter the operator's

display — making it more difficult to detect a new alarm and increasing the chances that the operator will respond incorrectly or miss a critical alarm.

A key metric to consider during this assessment is the rate at which the alarms are presented to the operator. In order to provide adequate time to respond, an operator should be presented no more than one to two alarms every 10 min. A related metric is the percentage of 10-min intervals during which the operator receives more than 10 alarms, which indicates the presence of an alarm flood. The ISA-18.2 standard's recommended targets for performance and diagnostic metrics are shown in Tables 2 and 3.

Table 2. ISA-18.2 recommends these targets for the number of alarms presented to the operator during each 10-min period, each hour, and each 24-h day.

Number of Annunciated Alarms per Operating Position per …	Target Value	
	Likely to be Acceptable	Maximum Manageable
Day	~ 150	~ 300
Hour	~ 6*	~ 12*
10 minutes	~ 1*	~ 2*
* For these metrics, averages should be calculated based on at least 30 days' data.		

Table 3. ISA-18.2 recommends these targets for performance and diagnostic metrics.

Metric	Target Value
Percentage of hours containing more than 30 alarms	<1%
Percentage of 10-min periods containing more than 10 alarms	<1%
Maximum number of alarms in a 10-min period	≤10
Percentage of time the alarm system is in a flood condition	<1%
Percentage contribution of the top 10 most frequent alarms to the overall alarm load	<1% (target), with a maximum of 5% Action plans are required to address deficiencies
Number of chattering and fleeting alarms	0 Action plans are required to correct any that occur
Number of stale alarms	Less than 5 present on any day Action plans are required to address excess alarms
Distribution of priorities of annunciated alarms	3 priorities: ~80% Low, ~15% Medium, ~5% High
	4 priorities: ~80% Low, ~15% Medium, ~5% High, <1%

	Highest Other special-purpose priorities are excluded when calculating the value of this metric
Number of unauthorized alarm suppressions (*i.e.*, outside of controlled or approved methodologies)	0
Number of unauthorized changes to alarm attributes (*i.e.*, outside of approved methodologies or MOC)	0

Performance targets are approximate and are based primarily on what an operator is capable of handling. The use of these targets as metrics for a particular plant, and the maximum acceptable numbers, will depend on many factors, including the type of process, operator skill level, HMI design, degree of automation, operating environment, and types and significance of the alarms generated. For example, acceptable rates for alarms related to safety or product quality in certain industries (*e.g.*, nuclear, pharmaceutical) are likely to be close to zero.

One of the most beneficial analyses is to routinely review the top 10 or 20 most frequently occurring alarms. In the absence of an effective alarm management program, these bad actors may contribute 50%–80% of the overall alarm load on the operator. Fixing these alarms represents low-hanging fruit for improving performance. Analyzing alarm system performance by class can provide valuable information. For example, it can identify whether any safety-critical alarms are being suppressed or behaving as nuisance alarms, both of which are indicators of a dangerous situation. One of the contributing causes to the accident at the DuPont Belle, WV, plant was the frequent false (nuisance) alarms generated by a burst disc sensor. The alarms from this sensor, which had been designated as OSHA-PSM- critical equipment, were ignored by operators because they had become accustomed to it behaving as a nuisance alarm *(5).*

Alarm management is a continuous process that is never finished. Measuring alarm system performance and taking action on the findings is an important ongoing activity and is critical to continuous improvement. An effective alarm philosophy documents the KPIs in a format that clearly defines target vs. unacceptable levels, the frequency of measurement and review, and the personnel responsible for taking action based on the results.

Stage 9: Management of Change

Even the most well-designed alarm system can experience problems if changes to it are not strictly controlled.

Management of change ensures that modifications to the alarm system, such as changing a setpoint or adding/ removing an alarm, are reviewed and approved prior to implementation. An effective MOC process balances the need for rigor and traceability with the need to make changes promptly to avoid impacts on production. For example, changing the limit for a safety-critical alarm may require a different level of review and authorization than changing the deadband of a general process alarm. Once a change is approved, the master alarm database should be updated and operators should be trained on the impact of the change.

The alarm philosophy should define the level of MOC that is required based on the type of change and the alarm's classification or priority. A contributing factor to the Deepwater Horizon drilling rig accident was the practice of disabling the annunciation of the general master alarm designed to notify personnel of danger (fire or explosive/ toxic gas), in order to prevent false alarms from waking personnel in the middle of the night *(7).* Perhaps if this alarm had been classified as personnel-safety-critical, the proper controls would have been in place to prevent it from being disabled.

Stage 10: Audit

During the audit phase, plant personnel conduct periodic reviews to assess actual alarm management work practices against the designed work practices outlined in the alarm philosophy. The goal is to maintain the integrity of the alarm system and to identify areas of improvement. Audit also includes a review of system performance, which may reveal gaps not apparent from alarm performance monitoring.

Operator interviews should be conducted to assess system performance from a human perspective — for instance, to verify that alarm priority is applied consistently. A recommended best practice is to periodically compare the running alarm system configuration with the master alarm database to ensure that unauthorized configuration changes have not been made.

Create an Effective Alarm Management Program

The hardest part of creating an effective alarm management program is getting started. Brownfield facilities (those with existing control systems) should start with either the monitoring and assessment or the audit stage. Facilities with new control systems (greenfield sites) should start by creating an alarm philosophy document and obtaining management approval.

Another critical success factor is structuring an alarm- management program that is realistic — one that emphasizes the ongoing nature of alarm management and that key personnel can commit to. Ideally, existing operational plants would complete alarm rationalization early in this effort, but the time and personnel requirements may preclude this. In some cases, it may be necessary to implement rationalization in stages.

An effective ongoing program includes a periodic review of alarm-system performance (*e.g.*, monthly), followed by prompt action to address any alarm system performance issues that are identified (Figure 5). Plants should constantly strive to improve performance as part of a continuous improvement initiative.

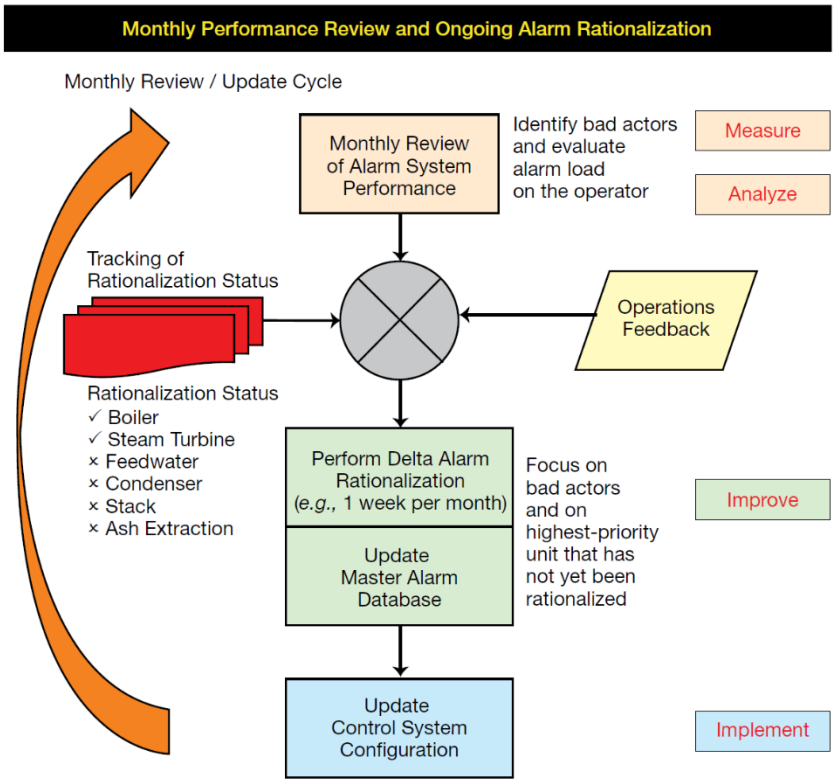

Figure 5: Ongoing alarm management should include a periodic review of alarm-system performance, followed by corrective actions when necessary

References

1. O'Brien, L., and D. Woll, "Alarm Management Strategies," ARC Advisory Group, Boston, MA (Nov. 2004).
2. The International Society of Automation, "Management of Alarm Systems for the Process Industries (ISA-18.2)," ANSI/ ISA 18.2–2009, ISA, Research Triangle Park, NC (June 2009).
3. Engineering Equipment and Materials Users Association, "Alarm Systems: A Guide to Design, Management and Procure- ment," 2nd ed., EEMUA 191, Engineering Equipment and Materials Users Association, London, U.K. (2007).
4. Zapata, R., and P. Andow, "Reducing the Severity of Alarm Floods," Proceedings of the Honeywell Users Group Americas Symposium 2008, Honeywell, Phoenix, AZ (2008).
5. U.S. Chemical Safety and Hazard Investigation Board, "E. I. DuPont de Nemours & Co., Inc.," Investigation Report 2010-6- I-WV, CSB, Washington, DC (Sept. 2011).
6. Buncefield Major Incident Investigation Board, "The Buncefield Incident 11 December 2005: The final reports of the Major Incident Investigation Board," Vol. 1, Buncefield Major Incident Investigation Board, London, U.K. (Dec. 2008).
7. Muskus, J., "Deepwater Horizon Alarm System Was Partly Disabled Prior To Explosion, Technician Tells Congress," *Huff- ington Post*, www.huffingtonpost.com/2010/07/23/deepwater- horizon-alarm-s_n_657143.html (Jul. 23, 2010).

ADDITIONAL READING

1. Stauffer, T., *et al.,* "Managing Alarms Using Rationalization, "*Control Engineering,* 58 (3), pp. 30–35 (Mar. 2011).
2. Stauffer, T., *et al.,* "Alarm Management and ISA-18 — A Journey, Not a Destination," Texas A&M Instrumentation Symposium, Available at www.exida.com/index.php/resources/whitepapers (Jan. 2010).
3. Stauffer, T., *et al.,* "Get a Life(cycle)! Connecting Alarm Man- agement and Safety Instrumented Systems," ISA Safety and Security Symposium, Available at www.exida.com/index.php/ resources/whitepapers (Apr. 2010).

Revision History

Authors: Todd Stauffer

exida – Who we are.

exida is one of the world's leading accredited certification and knowledge companies specializing in automation system cybersecurity, safety, and availability. Founded in 2000 by several of the world's top reliability and safety experts, exida is a global company with offices around the world. exida offers training, coaching, project-oriented consulting services, standalone and internet-based safety and cybersecurity engineering tools, detailed product assurance and certification analysis, and a collection of online safety, reliability, and cybersecurity resources. exida maintains a comprehensive failure rate and failure mode database on electrical and mechanical components, as well as automation equipment based on hundreds of field failure data sets representing over 350 billion unit operating hours.

exida Certification is an ANSI (American National Standards Institute) accredited independent certification organization that performs functional safety (IEC 61508 family of standards) and cybersecurity (IEC 62443 family of standards) certification assessments.

exida Engineering provides the users of automation systems with the knowledge to cost-effectively implement automation system cybersecurity, safety, and high availability solutions. The exida team will solve complex issues in the fields of functional safety, cybersecurity, and alarm management, like unique voting arrangement analysis, quantitative consequence analysis, or rare event likelihood analysis, and stands ready to assist when needed.

Training

exida believes that safety, high availability, and cybersecurity are achieved when more people understand the topics. Therefore, exida has developed a successful training suite of online, on-demand, and web-based instructor-led courses and on-site training provided either as part of a project or by standard courses. The course content and subjects range from introductory to advanced. The exida website lists the continuous range of courses offered around the world.

Knowledge Products

exida Innovation has made the process of designing, installing, and maintaining a safety and high availability automation system easier, as well as providing a practical methodology for managing cybersecurity across the entire lifecycle. Years of experience in the industry have allowed a crystallization of the combined knowledge that is converted into useful tools and documents, called knowledge products. Knowledge products include procedures for implementing cybersecurity, the Safety Lifecycle tasks, software tools, and templates for all phases of design.

Tools and Products for End User Support

- exSILentia® – Integrated Safety Lifecycle Tool

- PHAx™ (Process Hazard Analysis)
- LOPAx™ (Layer of Protection Analysis)
- SILAlarm™ (Alarm Management and Rationalization)
- SILect™ (SIL Selection and Layer of Protection Analysis)
- Process SRS (PHA based Safety Requirements Specification definition)
- SILver™ (SIL verification)
- Design SRS (Conceptual Design based Safety Requirements Specification definition)
- Cost (Lifecycle Cost Estimator and Cost Benefit Analysis)
- PTG (Proof Test Generator)
- SILstat™ (Life Event Recording and Monitoring)

- exSILentia® Cyber- Integrated Cybersecurity Lifecycle Tool
  - CyberPHAx™ (Cybersecurity Vulnerability and Risk Assessment)
  - CyberSL™ (Cyber Security Level Verification)

Tools and Products for Manufacturer Support

- FMEDAx (FMEDA tool including the exida EMCRH database)
- ARCHx (System Analysis tool; Hardware and Software Failure, Dependent Failure, and Cyber Threat Analysis)

For any questions and/or remarks regarding this White Paper or any of the services mentioned, please contact exida:

exida.com LLC

80 N. Main Street

Sellersville, PA, 18960

USA

+1 215 453 1720

+1 215 257 1657 FAX

info@exida.com