
# Tips for Starting an Alarm Management Program

**White Paper**

**exida**

**80 N. Main St.**

**Sellersville, PA**

**www.exida.com**

**April 2013**

exida White Paper Library

http://www.exida.com/Resources/Whitepapers

Copyright exida.com L.L.C. 2018-2020

## Introduction

Congratulations. You've been assigned the task of establishing an alarm management program for your facility. So where and how do you begin? This article presents four practical tips for starting an effective and sustainable alarm management program that conforms to the tenets of a relatively new process industry standard for alarm management published by ISA.

## Tip 1: Understand Alarm Management Terminology, Concepts

Plenty of good information on alarm management can be found on the Internet by searching for the terms "alarm management" and "alarm rationalization." Typically, searching on these terms yields so much information that it is easy to become overwhelmed and confused. Therefore, begin with the basics by becoming familiar with good engineering practices for alarm management (see Figure 1).

Until very recently, process plant owners, process control system manufacturers, and alarm subject matter experts have been practically on their own to coin their own terms and advocate their own alarm management concepts. For example, even basic notions had become highly inconsistent, such as the difference between an alarm and an alert, and the differences among alarm conditioning, suppression, shelving, and inactivation.

In 2009, ANSI/ISA-18.2-2009: Management of Alarm Systems for the Process Industries was published, also known as the ISA-18.2 standard. The ISA-18.2 standard helps to clear the confusion by providing clear definitions of the common terminology and helping to create a universal alarm management language. It also defines an alarm management lifecycle model, which establishes the recommended workflow processes. This lifecycle provides the central framework for understanding the requirements for building an alarm management program. Any products, services, or in-house processes that are put in place should be mapped against the model to identify gaps and assess compliance. Since the ISA-18.2 standard was published, most alarm solution vendors and industry alarm consultants have begun—or completed work—to align their offerings and solutions with the standard.

First, understand alarm management terminology and concepts according to the ISA-18.2 standard and then proceed to see what else the Internet has to offer.

## Tip 2: Clarify Top-Level Objectives, Program Scope

Quite possibly, your new task was motivated by a costly process disruption or maintenance expense caused by a poorly performing alarm system. There are also new and emerging business drivers for creating an alarm management program. ISA-18.2 is the first normative standard suitable for defining good engineering practices for alarm management in the process industries, which should be of interest to regulatory and insurance risk-rating bodies. By applying ISA-18.2 concepts, some companies expect to lower maintenance costs and achieve higher operating performance. For some companies, the business impact of an uncontained abnormal event is so severe that getting and keeping alarms under control is reason enough to create and maintain a standardized alarm management program.

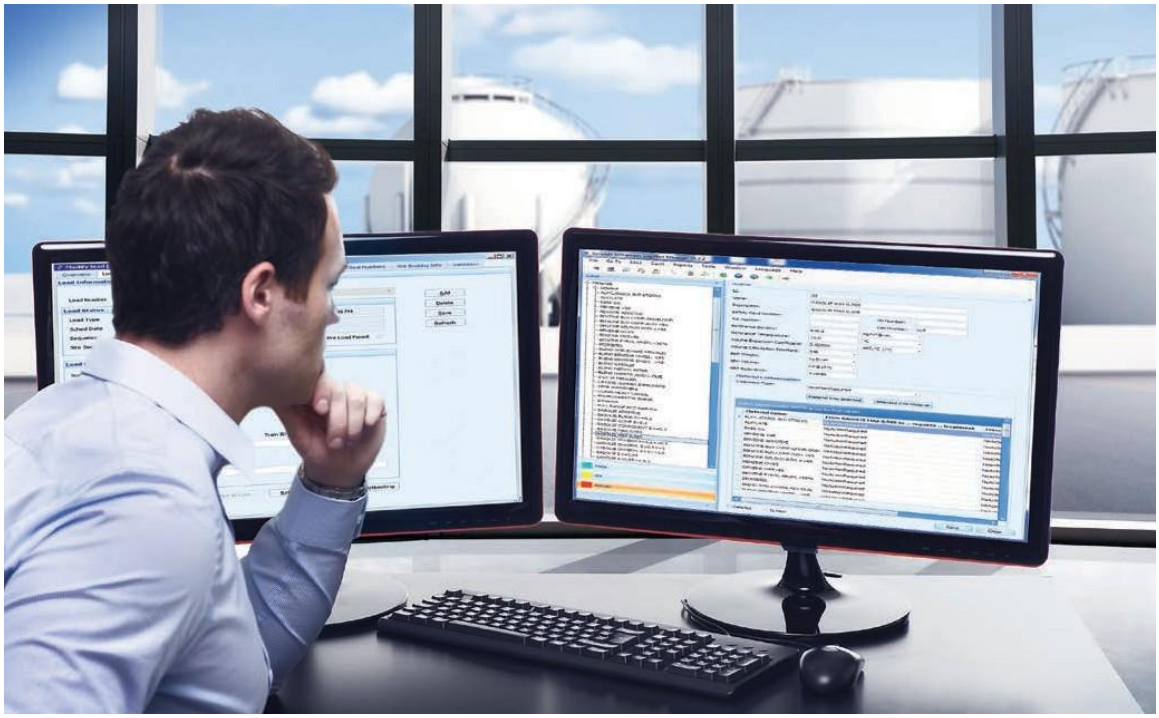
Establishing program goals is important because there should be a natural hierarchy to the scope of a successful alarm management program, which must be matched to the top-level objectives. Proceeding from least to greatest scope, this hierarchy includes:

- A limited program of nuisance alarm elimination
- Alarm rationalization with basic alarm redesign as required
- Advanced alarming techniques and operator HMI optimization.

***Eliminating nuisance alarms:*** Operators are often subject to nuisance alarms, which are alarms that annunciate excessively or unnecessarily, or do not return to normal after the correct response is taken (e.g., chattering, fleeting, or stale alarms). Prolonged exposure to nuisance alarms can desensitize the opera- tor to alarms and lead them to think it is acceptable to ignore alarms. Also, routine changes in the state of the process (start-up, shutdown, and out-of-service) often can result in alarms that are irrelevant based on the state of the process. However, they still clutter the alarm list. It is not unusual for up to 80% of all alarm activations to originate from a dozen or fewer sources. Thus a program of bad actor alarm identification and elimination can—with minimal effort—significantly quiet the control room, freeing operators from needless interruptions. This is just one activity in an effective alarm management program. There is a significant risk to limiting the scope of your program to only nuisance alarm elimination. When a real process disruption or equipment malfunction happens, it often leads to a flood of alarms of varying relevance and usefulness, with alarms prioritized in ways that do not truly reflect their importance. A program of only nuisance alarm rationalization does very little to help the operators cope with actual process disturbances beyond simply lowering the baseline level of background noise. Most alarm management experts caution that, while nuisance alarm elimination is a good thing, it does not equate with a true alarm management program.

***Alarm rationalization, basic alarm techniques:*** The ISA-18.2 standard specifies that an alarm should be reserved to indicate to the operator that an equipment malfunction, process deviation, or abnormal condition exists that requires a response. The implication is that for every alarm there is a defined operator action that will mitigate or prevent the likely consequences and sufficient time available for the operator to take the prescribed action.

Alarm rationalization is the process of reviewing potential—and existing—alarms using the guidelines defined in the alarm philosophy (a document you will create) to select alarms for design, and to document the rationale for each alarm. Alarm rationalization thus identifies which alarms to implement, or remove if there is insufficient basis, and their specifications such as priority, limit, and any conditioning such as on/off delays or hysteresis. Clearly, a systematic and careful review of all potential alarm sources, alarm design specification, and subsequent implementation in the control system is a major undertaking. However, this is the necessary investment if one of the top-level objectives is to ensure that the operator can respond decisively and consistently when actual process disruptions or equipment failures occur.



A good start to building a sustainable and effective alarm management program begins with a clear understanding of objectives and the basic principles of the alarm management lifecycle.

***Advanced alarm techniques, HMI redesign:*** Advanced alarming is a collection of techniques (e.g., state-based alarming and static/dynamic suppression) that can help manage alarm rates in specific situations. One example is to programmatically consolidate multiple alarm annunciations when a compressor or other large process asset trips offline to prevent the operator from being flooded with alarms and to make clear what has occurred. There may also be a need for special control displays to manage such an event. Perhaps a revamp of operator process displays is warranted to increase alarm visibility and promote greater situational aware- ness. The application of advanced alarming techniques and HMI redesign can represent significant effort and expense. Often, implementing certain advanced alarming techniques can be low-hanging fruit, such as online in-context presentation of alarm guidance based on information collect- ed during the alarm rationalization process. Implementation of advanced alarming and better HMI design can be expensive, so it may makes sense for it to be linked to a DCS upgrade or performance optimization project to deliver on its potential benefit. Clarify expectations with your management early, calibrating them to the costs and expected benefits, and scale your alarm management program accordingly.

## Tip 3: Build a Closed-Loop Process to Achieve, Sustain Positive Results

The fundamental concepts and benefits of a closed- loop process should be well understood. A close inspection of the alarm lifecycle model within the ISA-18.2 standard reveals its similarity to a closed-loop process with a setpoint and feedback mechanism (see Figure 2).

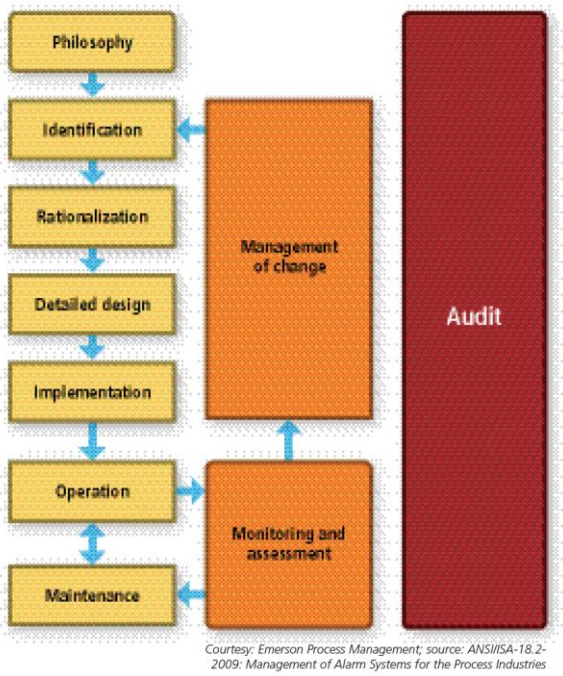



Figure 2: This diagram illustrates the ISA-18.2 alarm lifecycle model. The alarm management philosophy document is the setpoint for the process.

A good starting point is the creation of an alarm philosophy document, which serves as the setpoint for the alarm management process. This document establishes the principles and processes for design, implementation, and maintenance of the alarm system as well as its expected performance. An incomplete or inadequate alarm philosophy—or setpoint—will likely lead to confusion, unsustainable results, and alarm management system failure. For example, if the alarm rationalization activity becomes mired in lengthy discussions about each alarm's priority or need, determines that almost every alarm has a critical priority, or drifts over time in its approach to set- ting limits or applying conditioning, chances are high that the alarm philosophy is lacking. A good alarm philosophy, among other things, specifies the methodology for alarm prioritization, drives consistency, and includes the guiding tenets for determining all alarm settings.

The alarm philosophy defines the desired results, which are usually measured using key performance indicators (KPIs). Typical KPIs include:

- Alarm rate targets such as the average number of alarms per day per operator and the percentage of time the incoming alarm rate was greater than 10 alarms per 10 min. interval
- Maximum number of alarms that have been active for more than 24 hr
- Target alarm priority distributions such as an 80% to 15% to 5% ratio among the number of low-, medium-, and high-priority alarms.

For the closed-loop alarm management process, the alarm system performance should be measured periodically, converted to KPIs, and assessed. However, it's often more difficult to include effective management-supported organizational processes that:

- Systematically review the feedback to identify issues
- Maintain an effective management of change process that detects and prevents divergence between approved settings and actual (unauthorized) alarm set- tings in production
- Promote a continuous improvement program including removing or modifying the design of ineffective alarms.

It's important to put significant effort into creating the alarm philosophy. Be certain to involve and get the complete buy-in of all major stakeholders (operations, control engineering, and process engineering). It is often advantageous to enlist expert consultation services to assist with philosophy creation, training on alarm management practices and principles (to aid organizational alignment), and to facilitate some starter rationalization assistance.

## Tip 4: Acquire the Right Tools to do the Job

Finally, get the right tools to do the job. Building and sustaining an alarm management program represents a considerable and ongoing investment. The ISA-18.2 standard does not prescribe the methods for compliance; it defines only what must be accomplished. Fortunately, many good products and services are available to make it easier to implement an alarm management program in alignment with the standard and to deliver benefits to the bottom line.

An essential tool is a master alarm database, which is the authorized list of rationalized alarms and associated attributes. Its functionality can be achieved with no more than a simple spreadsheet or database. However commercial built-for-purpose tools include powerful aids for facilitation of the alarm rationalization process, including management of change mechanisms, guided workflows for efficiency, automated transfers of alarm settings and operator guidance into (or out of) the control system, auditing capabilities, and rationalization rule sets that can be populated with choices and KPI targets taken from your alarm philosophy.

Alarm analysis software is also essential for auto- mating KPI collection and reporting. If the top-level objective is limited solely to nuisance alarm elimination (which hopefully is not the case), it may be the only tool you require. Alarm analysis software typically provides a mix of KPI reporting capability based

on ISA-18.2's recommended performance metrics, some general-purpose alarm investigation aids to drill into an alarm flood or a particular alarm's history, and some bad-actor listing capability.

If the scope of the alarm management program includes advanced alarming techniques, additional tools may be required to implement presentation of alarm response procedures to operators or automate multi- alarm suppression schemes, for example.

Some alarm management tools are offered as combined or tiered software suites and are well suited for layered applications over widely varied control systems from different vendors. Some tools are offered as individual point solutions to satisfy particular elements of the alarm lifecycle model. Some alarm management solutions from control system vendors focus on optimizing native integration. Features, integration considerations, lifecycle costs, and initial price vary considerably. When making comparisons, it is helpful to associate the major features of each offering to the lifecycle model in the ISA-18.2 standard to ensure meaningful comparisons and to ensure you have all of the bases covered. In general, having the right tools will improve efficiency and help ensure long-term consistency of your alarm management program. The ISA-18.2 standard has had a positive impact on the evolution of these software tools.

In addition, the services offered by alarm management companies and individual consultants have also benefited from the ISA-18.2 standard. Evaluating the scope of professional service proposals can also benefit from comparing them to the lifecycle model.

## Revision History

**Authors:** Kim Van Camp, Todd Stauffer

Posted with permission from April 2013. Applied Automation, www.appliedautomationmag.com CFE Media. Copyright 2012. All rights reserved.

## *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