Think of alarm redesign as the building. The alarm philosophy is the foundation. Every time you want to change or add a seemingly small thing along the way, remember that it will need to conform to your design—the philosophy. Quickly, those small things can require significant modification to a philosophy that was developed along different lines. Everything built on the philosophy depends on it in some way or another. Not only is that dependence during design and construction—it will be for longer. It will be for as long as the alarm system is used.

### Owner versus Designer

The entire purpose of an alarm system is to provide effective operator support. At the end of the day, the operator's ability to understand, use, and benefit from any alarm system is the final test. Plant operations therefore owns the alarm system. However, "the ability to understand, use, and benefit from" does not necessarily mean that the owner is the best or even a qualified designer. After all, you are pretty much adept at using your automobile. You can easily decide which brand and model handles to your satisfaction. It is doubtful if you would be as effective at designing the fuel injection system. However, experts at designing fuel injection systems also drive automobiles.

Alarm systems are designed by those qualified and experienced in the technology. Operators have a vital role to play. Some may even lead the activity. Most times, it is a team comprised by operators, engineers, technicians, safety, and management personnel.[1]

### Reliance on Philosophy

There might come a time when an operator or engineer may be called on to "justify" (sometimes it is really *defend*) a decision or action. Management should understand that an appropriate reliance on the philosophy must be construed as evidence of good faith and acting with proper responsibility.

### Completeness

Items and lists provided in this book are suggestions for consideration. They are not exhaustive, of course. And you do not have to use them. But they should be well worth your consideration. The final list that each site develops will need to represent the best efforts of that site. It should cover those concerns and issues your site feels must be included in the alarm system design basis.

## 6.3 GETTING STARTED

Let's dig into this. We are at the solution part of the alarm improvement roadmap (fig. 6.3.1). The manufacturing team under the leadership of senior plant management develops the alarm philosophy. It describes the intended alarm design/redesign process from

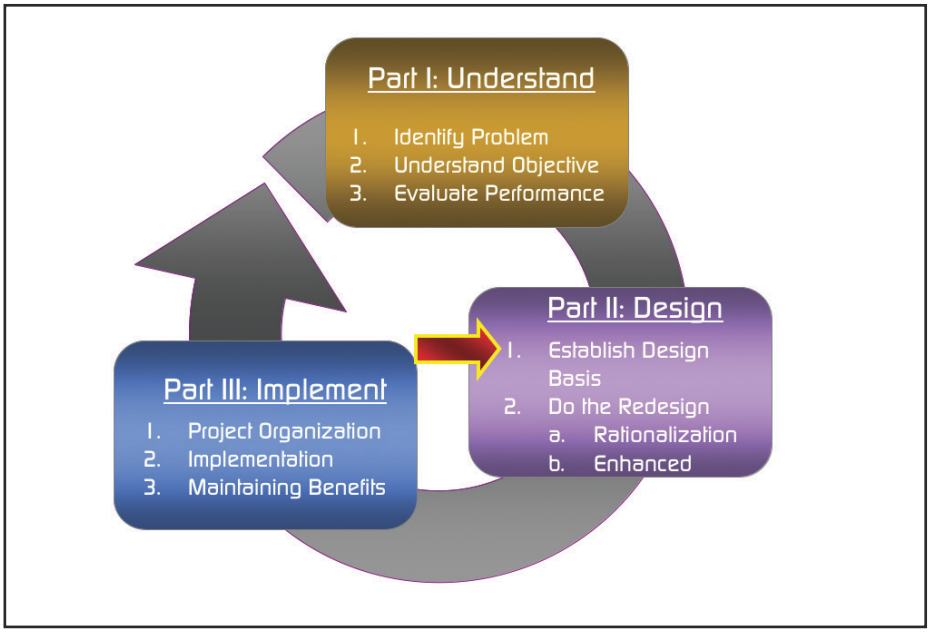


**Figure 6.3.1.** Roadmap location for philosophy

beginning to end. It starts with the buy-in of site management, progresses through the critical success factors, and includes the complete engineering design requirements to do the job well. It enables the provision for adequate financing, development of realistic schedules, and the inclusion of cooperation and participation from all the other key site players. The list of the detailed engineering design requirements will include the working definition of alarms; their proper response; other details of the alarm system; the integration with maintenance, training, and the remaining plant infrastructure; and the specific path to implementation. This will all provide postimplementation robustness and relevance.

## Operator Survey

The alarm system is a primary operator support tool. A good one can really assist the operator. A poor one is what you might have now. Many sites ask the operators how they think their current alarm system is working. There is a formal survey form that EEMUA 191[2] recommends. A revised version is shown in appendix 3.

## Advice to the Reader on Timing of This Topic

The discussion of alarm philosophy comes quite naturally at this juncture in the development of effective alarm system designs. However, it is suggested that you delay a bit

more before actually preparing one. In other words, please wait until you have read and understood what this book is all about before you set out to do the important task of developing your own alarm design by developing a philosophy.

## 6.4 SPECIAL ALARM ISSUES

### Types of Alarms and Their Recommended Use

Conventional PCS controller loops can configure many types of process alarms. The following are examples:

- High absolute
- Low absolute
- High-high absolute
- Low-low absolute
- High deviation
- Low deviation
- High rate of change
- Low rate of change

All these types are useful. Each provides a certain specialty that will be just right for some situations. Which ones to you will want to use and for what purpose, generally falls into one of the three categories discussed below. There are exceptions, of course.

#### *Normal Process Abnormalities*

*High* and *low* in this discussion refer to the directionality for approaching the abnormal situation, not anything else. The high and low absolute alarms are the workhorse of alarm systems. They are used to signal events that are enough out of the ordinary to require operator interventions. The high-high and low-low absolute alarms are reserved for the unusual situations where the few normal abnormalities can suddenly, and without the usual warning, escalate to the very serious. This escalation would only happen during the normal course of the operator working to resolve the current alarm. Once the situation has escalated, the consequences and operator actions change dramatically. For all other cases, the high-high and low-low alarms would be redundant with the high and low alarms—therefore, they would be unnecessary. Please also refer to "Special Cases of Redundant Alarms" below.

#### *Incipient Process Abnormalities*

Incipient abnormal situations are those where the process slowly approaches an abnormal situation. It is the very act of the slow movement that makes the situation difficult

for the operator to notice. And since it is slow, the total amount of movement is small. Before an absolute alarm limit could be exceeded, the plant would be in serious trouble. These situations are usually best identified by rate-of-change alarms. As the process moves toward the abnormal, the rates of change usually increase.

### *Processes that Move a Lot*

There are some processes that change their production aspects quite a bit during a normal production cycle. The production requires close attention, but the attention points are always moving about. One way to track the abnormal situations is to watch for abnormal excursions from normal. Deviation alarms are ideally suited for this purpose.

## Smart Field Devices

Besides improved functionality and ease of application, smart field devices also incorporate significant diagnostic ability. Most of the diagnostics track device degradation and alarm them long before the device fails. Most, if not all, of these diagnostics are of little value to the operator—but extremely relevant to maintenance personnel. Current practice is not to configure operator alarms for these but to allow the PCS to route them to maintenance personnel directly.

## Light Boxes

Light boxes are the colloquial term used to describe those individual alarms that are announced by dedicated electronic hardware separate from the PCS. The usual form is a wall- or panel-mounted illuminated engraved window that will light and sound a hardware horn whenever the point goes into alarm. Some use differing colors for the window or lightbulb to indicate alarm severity. They occasionally use different sounds for the horn to do the same.

If light-box alarms are meant for the operator (our operator in the operator area), then light-box alarms are handled just like any other alarm, with the exception that they are usually considered to be a "required alarm." But even required alarms are examined to ensure that the priority is correct, the activation point is correct, and the appropriate operator support documentation and training is in place.

## Special Cases of Redundant Alarms

After all is said and done for a properly designed alarm system, you will notice that an entire class of alarms that might have been used before is not to be found now. You will note that there are no (or very, very, very few) prealarms. You won't very often find a high alarm and then a high-high alarm. Nor will you find low and then a low-low. This is not an accident. It goes back to our fundamental precepts underlying alarms.

Before alarm redesign, the reason that plants used both a prealarm and an alarm were to ensure that a few important situations were not missed by (a) announcing the problem early and then (b) confirming that the problem still existed later on as it persisted. The prealarm (the high or low) was provided to alert the operator that there was a problem. The follow-on alarm (high-high or low-low) was provided to let the operator know that the problem (which might have or might not have been seen or worked on earlier) is still there and getting worse. After the activation of the follow-on alarm, it was expected that operator action take place, usually serious operator action. So far, this all sounds good. The failure becomes obvious when we think about what should be done to configure the prealarm and the follow-on alarm, using our newfound approach to effective alarm design.

Consider the follow-on alarm first. Properly designed, this alarm would require operator action and must alert the operator with enough time remaining for good operation to be restored. During the process of restoring good operation, we expect our operator to keep a continual eye on what's going on and remain aware of how things are progressing. Since, by design, the operator should be able to manage this abnormal situation from the time the alarm activated, there is nothing to be gained by alerting earlier. Nor should we assume that the *process safety time* is any less, nor the *time to manage fault* any longer, for the follow-on alarm than would be the case for any prealarm. If anything, the follow-on alarm would represent a more serious situation. As such, it is reasonable to expect both the time for diagnostic effort and the plant response time to be longer than they might be for a less-serious prestate. Consequently, a prealarm represents nothing more than a redundant alarm. It should not be used. You should very rarely see high-high or low-low alarms.

## About Alerts

Prealarms are not such a good idea. To replace them, we might be tempted to provide much the same functionality by using an alert. Chapter 12 presents an illustration of the alert concept. Alerts aren't alarms, so we won't have any redundancy to worry about. As things start to get bad, we just issue an alert for each case. Sounds like a good way to have our way. Or is it?

Alerts are meant to convey messages to the operator without (improperly) having to resort to alarms. But alerts are important in their own right. They convey important information that the operator needs to stay on top of things. And just like any other tool, if it is used in a way not intended and for which it is ill suited, it becomes less able to do what it was intended for. If we were to use alerts to provide prealarm warnings for "important" alarms, we would generate a lot of alerts. In effect, we would be trading alarm overload for alert overload. Overload is overload. Maybe the best thing is to avoid the prealarm conundrum altogether and trust in our alarm design to do what we designed it do to.

Many PCS systems do not provide even a rudimentary messaging or alert type of functionality. In order to remove all the alarms that are present in an unimproved alarm

system, it may be necessary to use a workaround. If the PCS alarm system has one or more alarm priority levels that are not required for operator alarms and it permits those alarms to be (a) routed to places other than the operator's station and (b) configured so they will not sound the operator's horn, then those extra priority levels may be used as alerts. None of these alerts is counted as or treated as an alarm in the philosophy or anywhere else. As simple as this all appears, and it really is, some rationalization practices fail to understand the importance. Please remember this when you read about *partial rationalizations* in chapter 7. None are acceptable.

Yet, there is good reason for having a way to notify operators of things that he might find useful, even important, to know. The general terms for these are called *notifications*, *messages*, or *alerts*. Most PCS vendors are working hard to provide some useful messaging capability to their systems. Please have a look at Appendix 11 for more background on this subject if you are interested.

### Classes of Alarms

There is a movement among alarm practitioners to categorize alarms beyond required and ordinary. Typical extra categories are *highly managed* and *safety*. Those practitioners go as far as suggesting that they be configured and operated differently from the required and ordinary ones. Please resist this movement. It is not needed. It is an unnecessary complication that provides a bit of comfort at the expense of good alarm practices.

In a properly configured alarm system, alarm importance is built in. For most plants, abnormal operation can result from missed low-priority alarms as well as from missed high-priority ones, from alarms that derive their importance from financial impacts as well as those that relate to environmental or safety ones. Any attempt to overlay the best practices with additional alarm complication will only serve to confuse the operator and unnecessarily complicate a well-designed alarm improvement process.

## 6.5 OVERVIEW OF ALARM PHILOSOPHY

The redesign of an alarm system will necessarily impact a number of the entrenched parts of the existing plant infrastructure. A one-size-fits-all approach usually does not work very well here. Every plant has its own history, its own way of doing things, its own problems, its own goals, and its own style. So that all of those diverse aspects can be managed well, the chapter on alarm philosophy has been designed to bring out the really critical ones. The plant will decide what and if to include and how it will be done. With that disclaimer in place, you will find lots of reminder lists of items that usually are considered in most philosophy designs. You should find them quite useful. They help to ensure that something important is not inadvertently left out. As we start this coverage, please consider that the philosophy can only contain what is put into it. All assumptions, all preconditions, and all other parts that you want to think of as being there should not

be left up to chance. Lay them out and include them specifically into the document you will prepare.

## Philosophy 101

Before you get started with any alarm improvement project, it is important to recognize the fundamental aspects underlying successful process management. These will form the foundation of the design assumptions. They should be included in your document. They should be fully specified and explained, including specific action items that support them. The alarm improvement teams can only suggest the explicit arrangements that will be needed to adequately cover nonalarm items. They are included as part of your alarm redesign philosophy, not only for use of the alarm improvement teams, but also for the entire enterprise. The other steps necessary to ensure that the needed coordination is done should be assigned to others in the plant who normally deal with the particular infrastructure item. Example items include maintenance practices, general training practices (as opposed to alarm redesign training), operating procedure revisions, and the like.

The following items are the key bases to cover. The material illustrated in each part conveys helpful suggestions about what to include as well as what others have found to be a best practice. Your site will use them, modify them to suit, or develop others in their place. Your alarm philosophy will define and clarify each of the items that follow.

## Operator-Centric Items

- *Responsible operator*. The alarm system is not intended to take the place of proper operator management of the process or the operator's constant, watchful eye and exercise of insightful judgment.
- *Qualified operator*. Operators will be fully qualified and appropriately trained and monitored (performance, physical health, emotional and psychological health) for the job.
- *Operator ownership*. Alarms and alarm system are for the operator, not maintenance, not the safety department, and not the environmental department.
- *Alarms mean action*. All alarms will be responded to in a timely and appropriate manner.
- *Activations provide sufficient time*. All alarms should provide sufficient time for the operator to manage the process abnormality.
- *Priority guides*. Alarm priority will be used to guide the operator's order of attention to alarm activations.
- *Alarm response information*. Appropriate information will guide the operator to understand the abnormal situation and help decide and implement remediation actions.

- *Appropriate design.* Alarms will not be used to compensate for poor process design, poor equipment, inadequate maintenance, weak or ineffective procedures, and inadequate personnel training and readiness.

## Plant-Centric Items

It is assumed that the plant has been designed with due care. Its construction and operation are proper and according to plan. Therefore the alarm system itself should not be used to patch up, accommodate, or otherwise make up for inherent plant design inadequacies, maintenance inadequacies, poor procedures, unduly stressful operations, operation outside of proper design conditions, and the like. If the plant shares this view, then it is important to make sure that the alarm system is designed to be consistent with the primary understandings. Moreover, it is essential that the entire plant team recognizes this and takes the necessary steps to modify practices and standards to ensure that the plant is in condition to take proper advantage of the alarm system.

*Broken and missing equipment.* All equipment that is part of the plant and used for production shall be replaced if missing and fully repaired if operationally impaired or broken. If certain equipment has ongoing and unavoidable operational problems and therefore cannot be rendered fully operational during production, then specific procedures must be in place to handle this situation. Those procedures must include the operation of the alarm system during this situation. Training and controls must be modified to include proper accommodation of this situation. It must not be left to the alarm system to identify and moderate such situations.

*Unusual plant operation.* The plant has a design basis and an approved operating envelope. The alarm system will have been designed with that in mind. If the plant will be operated outside proper limits, for whatever reason, proper MOC should be used rather than reliance on the alarm system. While alarms might be important and useful, they have not been explicitly or implicitly designed for such operation. Therefore it is likely that activation points, priority, and other alarm information and performance may not be adequate.

*Unusual plant situations.* Plant manning and operating procedures have been developed and approved based on the plant practice and needs of operation. Any significant departure from these expectations shall not rely on the alarm system for adequate operation. Unusual situations include the following: operating during severe weather or other unusual natural situations, operating or attempting to operate during severe manpower shortages (perhaps due to illness, weather, or other emergencies), operating or attempting to operate with marginal or otherwise unsuitable or untested raw materials or other resources, and operating with marginal or untrained personnel or management.

*Recognition of limitations of alarm system operation.* Unlike safety systems and other key infrastructure components that have been designed and implemented to provide unambiguous operation under all conditions and situations, alarm systems are not. Alarm systems must not be relied on to cover all situations and accommodate to all insults. Careful attention should be directed to uncover missing safety systems and other

safety infrastructure to avoid any undue implicit reliance on the alarm system to keep the plant and personnel safe.

## Alarm System Purpose

The purpose of the alarm system is to bring a potentially abnormal process condition to the attention of the operator in time for appropriate remediation and with appropriate guidance for success. In the event that the operator suspects or is already aware of the possible existence of an abnormal situation or condition, the alarm system shall provide confirmation for those concerns.

One might observe that the alarm system is the presafety shutdown system. Thus the alarm system provides the last clear chance for plant operations to restore good operation before the plant is forced to end operation. As such, it offers a productive way to appropriately support the enterprise.

## Philosophy Intent

The alarm philosophy is, in the simplest of explanations, a complete design requirements list of how the alarm system is supposed to be designed and operated. It will *not* explain how to construct a project, how to estimate costs, how to man the work, or which vendors to approach to assist you. Its sole purpose is to describe the end result in as careful a way as possible. Here are some of the key parts to include.

*Needs evaluation.* The needs evaluation is an examination of the performance of the current plant to identify where it stands against the requirements for proper design and operation. This part must address what measurements are to be made, how they are to be done, what constitutes meeting the desired performance requirements (KPIs), and how to interpret the results in such a way as to provide action guidance and change requirements.

*Design.* The design will include what the new alarm system should look like, how the detailed redesign specification should be constructed, how changes in the other parts of the plant necessary to support the alarm redesign are coordinated, and how the new alarm system is to be produced.

*Implementation.* Implementation will cover all aspects of bringing the new alarm system to life and ensure that it fits in with the rest of the site infrastructure. Included are operations practices, procedures, revisions, training, documentation, MOC requirements, and the assignment of responsibility for the entire supporting infrastructure changes into the appropriate hands.

*Validation.* No new design is done until it is proven to perform as designed. How the new system will be proved shall be specified. Require all inadequacies to be addressed according to procedures laid down in the philosophy. The methodology for handling any uncured or incurable performance is also specified here. *A validated alarm system is one that has been shown to match the design requirements.*

*Auditing*. No new design is effective unless it is shown to resolve the issue that prompted it. Here is where the performance of the redesigned alarm system will be measured and compared against the requirements. Not only will the project goals be audited, but also the resulting performance must be validated against the project targets. For example, does the alarm system interfere with the operator's understanding of abnormal process operation? Does the alarm system appropriately guide the operator to understand and manage alarms? Is the alarm system a distraction during normal operation? Inadequacies will be addressed and remedied. Here is where all such requirements are specified. *An audited alarm system has been shown to meet the actual needs of the plant, whether or not those needs were adequately expressed in the design requirements.*

*Maintaining*. What works today may not necessarily work tomorrow. Here is where the plans are laid down and enforced so that the alarm performance will consistently deliver the required benefits into the future. Here is where we make sure that there are appropriate requirements for continued auditing, for auditing after incidents, and for auditing after modifications and any other events likely to impact the design or performance of the alarm system.

## Elements in the Philosophy

The following list highlights the key areas that the alarm philosophy should cover to guide design decisions:

- *Alarm design principles*. What specifically defines alarms? How should they be set up? How should they be interpreted and incorporated into the operator's kit?
- *Key performance indicators and critical success factors*. What important requirements need to be met for a proper alarm system design? How will we audit for proper performance?
- *Approved management of change requirements*. Do the modifications, additions, and changes to the existing MOC requirements include alarm management? Is the alarm system as well as the greater controls and operations support infrastructure appropriately secure against reckless and nefarious attacks and other insults?
- *Process for rationalization*. Specifically, what will be the recommended approach to be used to arrive at the requisite number of properly configured alarms?
- *Activation point determination*. Exactly what will be the procedure used to set the alarm activation point values?
- *Priority assignment*. How will priority be used and assigned to each alarm?
- *Alarm presentation*. How will each alarm be shown to the operators? How will operators locate the needed information to effectively deal with the alarm?
- *Enhanced alarming*. What logic and other controls will be put into place to ensure that each alarm activation properly reflects the current plant state and operations need?

- *Operator roles.* What is the operator expected to do before, during, and after alarm activations?
- *Interplay with procedures.* How will procedures reflect the alarm system? How will the proper use of the alarm system be represented in procedures?
- *Training.* How will training be modified to accommodate the new alarm system design? How will the new alarm system design rely on training?
- *Escalation.* When things go wrong, what is the plant's expectation for alerting others, obtaining additional assistance, changing operating goals, and shutting down or "parking" the plant?
- *Maintenance.* What are the maintenance requirements for the new alarm system design, both for the alarm system and for the rest of the plant?
- *Support/technology required in addition to the alarm system.* There are a number of key aspects of operation that need to be recognized and provided for that cannot be provided by the alarm system itself (or which currently depend on the alarm system, but should not). These are very important in their own right. To the extent that alarms will no longer provide information or support for these activities (even though they were done ineffectively), other ways to provide this support must be identified by the philosophy. The short list of these items includes (a) messaging, (b) true operating condition or status of plant, (c) tracking event escalation and migration (to other operator areas), and (d) system alarms for both process-related aspects (sensors, transmitters, etc.) and nonprocess aspects (storage, data highway loading, etc.). Refer to chapter 10 for a more complete discussion.

## 6.6 ALARM PRIORITY

**Important Message**

Pay particular attention to the definitions you will use for scoring each alarm in the area of *consequences and severities.* You will be doing the scoring for each alarm—which means thousands will be done. Since the priority distribution of the result will not be known until that work is well underway or complete, you will want to be sure that your definitions are correct. For if they are changed, then all alarms that were categorized before will need to be redone.

With consistent definitions, it is possible to modify priorities en masse simply by adjusting the consequences, severities, and urgency map to priority. This is the power of using tools.

Alarm priority is a clear and powerful way to expose and manage operational risk. Alarm priority encapsulates the urgency and impact effects of what will happen if the abnormal