Setting a new standard in alarm management

How to follow the ISA 18.2 alarm management standard to create a safer and more productive plant

www.usa.siemens.com/process

SIEMENS

Summary

Alarm management affects the bottom line. A well-functioning alarm system can help a process run closer to its ideal operating point – leading to higher yields, reduced production costs, increased throughput, and higher quality, all of which add up to higher profits. Poor alarm management, on the other hand, is one of the leading causes of unplanned downtime and has been a major contributor to some of the worst industrial accidents on record. Changing the practices and procedures used in the plant has become easier and more important with the release of a new ISA standard on alarm management. The ISA-18.2 standard, which provides a blueprint for creating a safer and more productive plant, is expected to be adopted by OSHA and insurance agencies as "good engineering practice." This paper provides an overview of the new standard and examples of how to follow it. The paper also describes the most important capabilities that a process automation system should provide in order to receive the most benefit from following the standard. A checklist of these key alarm management features is included at the end of the paper.

Contents

1.0 Introduction – Why alarm management is important

The global recession hurt the bottom line for many manufacturers in the process industries. Focusing on operational excellence is a key to short-term survival and to future growth. Poor alarm management is a major barrier to reaching operational excellence. It is one of the leading causes of unplanned downtime, which can cost $10K/hr to $1M/hr for facilities that run 24 x 7. It also impacts the safety of a plant and its personnel, having played a major part in the accidents at Three Mile Island (PA), the Milford Haven Refinery (UK), Texas City Refinery (TX), and the Buncefield Oil Depot (UK), which all resulted in significant cost - injury, loss of life, equipment and property damages, fines, and damage to company reputations.

At the Buncefield Oil Depot, a tank overflow and resultant fire caused a $1.6B loss. It could have been prevented if the tank's level gauge or high level safety switch had notified the operator of the high level condition.[1] The explosion and fire at the Texas City refinery killed 15 people and injured 180 more. It might not have occurred if key level alarms had not failed to notify the operators of the unsafe and abnormal conditions that existed within the tower and blowdown drum. [2]

In June of 2009 the standard ANSI/ISA-18.2-2009, "Management of Alarm Systems for the Process Industries", was released. This paper reviews ISA-18.2 and describes how it impacts end users, suppliers, integrators, and consultants. It also provides examples of the tools, practices, and procedures that make it easier to follow the standard and reap the rewards of improved alarm management.

2.0 The purpose of the ISA standard

ISA-18.2 provides a framework for the successful design, implementation, operation, and management of alarm systems in a process plant. It builds on the work of other standards and guidelines such as EEMUA 191, NAMUR NA 102, and ASM (the Abnormal Situation Management Consortium). Alarm management is not a "once and done" activity, rather it is a process that requires continuous attention. Consequently, the basis of the standard is to follow a life-cycle approach as shown in Figure 1.

The connection between poor alarm management and process safety accidents was one of the motivations for the development of ISA-18.2. Both OSHA and the HSE have identified the need for improved industry practices to prevent these incidents. Consequently, ISA-18.2 is expected to be "recognized and generally accepted good engineering practice" (RAGAGEP) by both insurance companies and regulatory agencies. As such, it becomes the expected minimum practice.

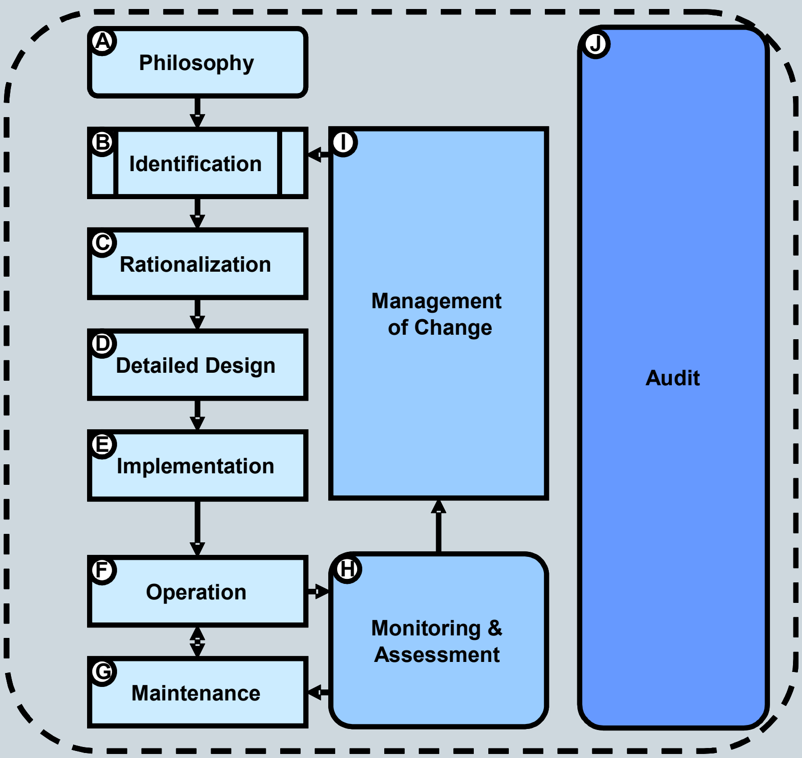


Figure 1 The alarm management life-cycle[3]

3.0 Common alarm management problems

Reviewing the definition of an alarm is helpful to understand its intended purpose and how misapplication can lead to problems.

> ***Alarm:*** *An audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a response.*

Figure 2 – Definition of alarm from ISA18.2 [3]

One of the most important principles of alarm management is that an alarm requires a response. This means if the operator does not need to respond to an alarm (because unacceptable consequences do not occur), then the point should not include an alarm. Following this cardinal rule will help eliminate many potential alarm management issues. The recommendations in the standard provide the "blueprint" for eliminating and preventing the most common alarm management problems, such as those shown in Table 1.

Alarm Management Problem	Cause(s)
Alarms are generated which are ignored by the operator.	"Nuisance" alarms (chattering alarms and fleeting alarms), faulty hardware, redundant alarms, cascading alarms, incorrect alarm settings, alarms have not been rationalized.
When alarms occur, operators do not know how to respond.	Lack of training and insufficient alarm response procedures
Minor plant upsets generate a large number of alarms.	Average alarm load is too high. Redundant alarms, cascading alarms, alarms have not been rationalized.
The alarm display is full of alarms, even when there is nothing wrong.	"Nuisance" alarms (chattering alarms and fleeting alarms), faulty hardware, redundant alarms, cascading alarms, incorrect alarm settings, alarms have not been rationalized.
Some alarms are present on the alarm display continuously for long periods of time (>24 hours).	Corrective action is ineffective, equipment is broken or out of service, change in plant conditions.
During an upset, operators are flooded with so many alarms that they do not know which ones are the most important.	Incorrect prioritization of alarms. Not using advanced alarm techniques (e.g. state-based alarming).
Alarm settings are changed from one operator to the next.	Lack of management of change procedures

Table 1 – Common alarm management problems that can be addressed by following the alarm management life-cycle of ISA-18.2

4.0 Overview of the standard and how to follow it

4.1 Philosophy (Phase A)

The first phase of the alarm management life-cycle focuses on the development of an alarm philosophy document. This document establishes the standards for how your company or site will address all aspects of alarm management - including design, operations, and maintenance. It should contain the rules for classifying and prioritizing alarms, for using color to indicate an alarm in the HMI, and for managing changes to the configuration. It should also establish key performance benchmarks, such as the acceptable alarm load for the operator (average number of alarms / hr). For new plants, the alarm philosophy should be fully defined and approved before commissioning. Roles and responsibilities for those involved in the management of alarms should also be clearly defined.

4.2 Identification and rationalization (Phases B and C)

In the second part of the alarm management life-cycle, potential alarms are identified. There are many different sources for identifying potential alarms including P&IDs, operating procedure reviews, process hazards analysis (PHA), HAZOPs, incident investigations, and quality reviews.

Next, these candidate alarms are rationalized, which means each one is evaluated with a critical eye to justify that it meets the requirements of being an alarm.

- Does it indicate an abnormal condition?
- Does it require an operator action?
- Is it unique (or are there other alarms that indicate the same condition)?

Alarms that pass this screening are further analyzed to define their attributes (e.g. limit, priority, classification, and type). Alarm priority should be set based on the severity of the consequences and the time to respond. Classification identifies groups of alarms with similar characteristics (e.g. environmental or safety) and common requirements for training, testing, documentation, or data retention. Safety alarms coming from a Safety Instrumented System (SIS) are typically classified as "highly managed alarms". These alarms should receive special treatment particularly when it comes to viewing their status in the HMI.

Alarm attributes (i.e. settings) are documented in a Master Alarm Database, which also records important details discussed during rationalization - the cause, consequence, recommended operator response, and the time to respond for each alarm. This information is used during many phases of the life-cycle. For example, many plant operations and engineering teams are afraid to eliminate an existing alarm because it was "obviously put there for a reason". With the Master Alarm Database, one can look back years afterward and see why a specific alarm was created (and evaluate whether it should remain).

Documentation about an alarm's cause and consequence can be invaluable to the operator who must diagnose the problem and determine the best response. The system should allow the alarm rationalization information to be entered directly into the configuration (e.g. as an alarm attribute) so that it is part of the control system database and so that it can be made available to the operator online through the HMI.

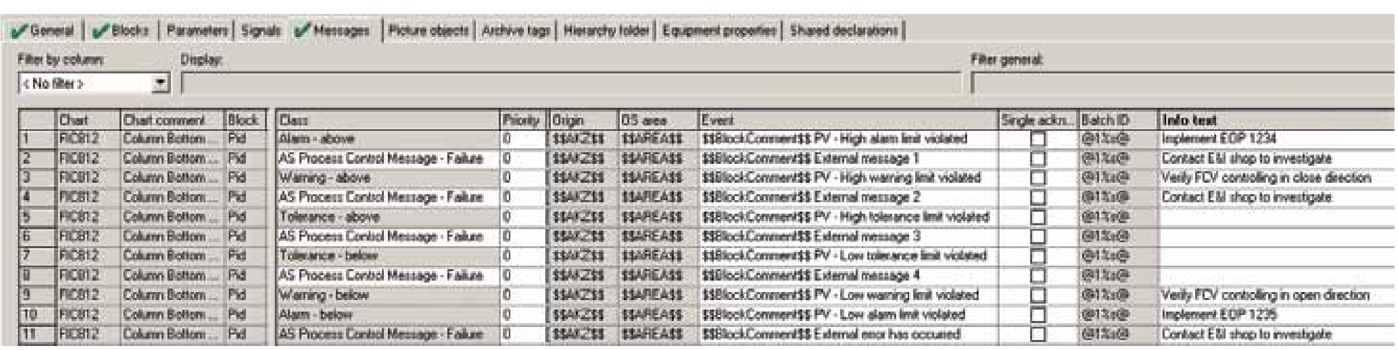


	Chart	Chart comment	Block	Class	Priority	Origin	OS area	Event	Single ackn.	Batch ID	Info text
1	FIC812	Column Bottom ...	Pid	Alarm - above	0	$$AKZ$$	$$AREA$$	$$BlockComment$$ PV - High alarm limit violated	☐	@1%s@	Implement EOP 1234
2	FIC812	Column Bottom ...	Pid	AS Process Control Message - Failure	0	$$AKZ$$	$$AREA$$	$$BlockComment$$ External message 1	☐	@1%s@	Contact E&I shop to investigate
3	FIC812	Column Bottom ...	Pid	Warning - above	0	$$AKZ$$	$$AREA$$	$$BlockComment$$ PV - High warning limit violated	☐	@1%s@	Verify FCV controlling in close direction
4	FIC812	Column Bottom ...	Pid	AS Process Control Message - Failure	0	$$AKZ$$	$$AREA$$	$$BlockComment$$ External message 2	☐	@1%s@	Contact E&I shop to investigate
5	FIC812	Column Bottom ...	Pid	Tolerance - above	0	$$AKZ$$	$$AREA$$	$$BlockComment$$ PV - High tolerance limit violated	☐	@1%s@	
6	FIC812	Column Bottom ...	Pid	AS Process Control Message - Failure	0	$$AKZ$$	$$AREA$$	$$BlockComment$$ External message 3	☐	@1%s@	
7	FIC812	Column Bottom ...	Pid	Tolerance - below	0	$$AKZ$$	$$AREA$$	$$BlockComment$$ PV - Low tolerance limit violated	☐	@1%s@	
8	FIC812	Column Bottom ...	Pid	AS Process Control Message - Failure	0	$$AKZ$$	$$AREA$$	$$BlockComment$$ External message 4	☐	@1%s@	
9	FIC812	Column Bottom ...	Pid	Warning - below	0	$$AKZ$$	$$AREA$$	$$BlockComment$$ PV - Low warning limit violated	☐	@1%s@	Verify FCV controlling in open direction
10	FIC812	Column Bottom ...	Pid	Alarm - below	0	$$AKZ$$	$$AREA$$	$$BlockComment$$ PV - Low alarm limit violated	☐	@1%s@	Implement EOP 1235
11	FIC812	Column Bottom ...	Pid	AS Process Control Message - Failure	0	$$AKZ$$	$$AREA$$	$$BlockComment$$ External error has occurred	☐	@1%s@	Contact E&I shop to investigate

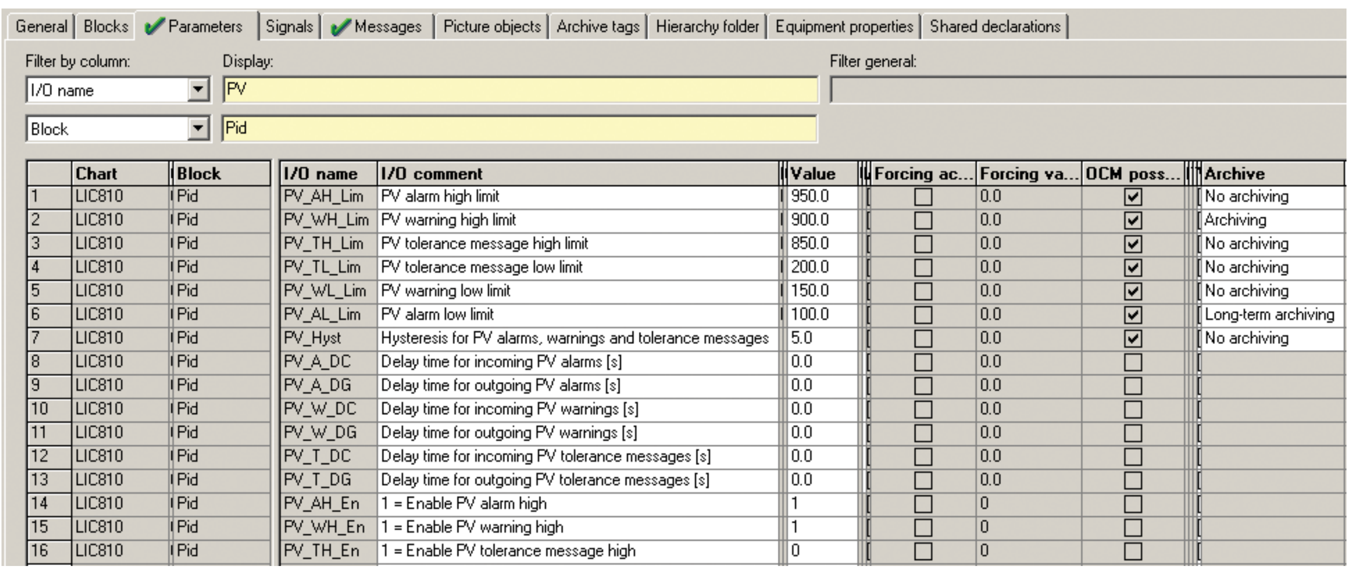
Figure 3 Entering cause, corrective action information from rationalization directly into PCS 7

One of the major benefits of conducting a rationalization is determining the minimum set of alarm points that are needed to keep the process safe and under control. Too many projects follow an approach where the practitioner enables all of the alarms that are provided by the DCS, whether they are needed or not, and sets them to default limits of 10%, 20%, 80%, and 90% of range. A typical analog indicator can have six or more different alarms configured (e.g. high-high, high, low, low-low, bad quality, rate-of-change, etc.), making it easy to end up with significantly more alarm points than are needed. To prevent the creation of nuisance alarms and alarm overload conditions, it is important to enable only those alarms that are called for after completing a rationalization. Thus an analog indicator, for example, may have only a single alarm condition enabled (e.g. high).

4.3 Detailed design (Phase D)

Poor design and configuration practices are a leading cause of alarm management issues. Following the recommendations in the standard can go a long way to eliminating the issues. In many control rooms, more than 50% of standing alarms are for motors (pumps, fans, etc.) that are not running.

During the detailed design phase, the information contained in the Master Alarm Database (such as alarm limit and priority) is used to configure the system. Alarm settings should be copied and pasted or imported from the Master Alarm Database directly into the control system configuration to prevent configuration errors. Spreadsheet style engineering tools can help speed the process, especially if they allow editing attributes from multiple alarms simultaneously. If the control system configuration supports the addition of user-defined fields, it may be capable of fulfilling the role of the Master Alarm Database itself.


General | Blocks | Parameters | Signals | Messages | Picture objects | Archive tags | Hierarchy folder | Equipment properties | Shared declarations

Filter by column: I/O name — Display: PV — Filter general:

Block — Pid

	Chart	Block	I/O name	I/O comment	Value	Forcing ac...	Forcing va...	OCM poss...	Archive
1	LIC810	Pid	PV_AH_Lim	PV alarm high limit	950.0	☐	0.0	☑	No archiving
2	LIC810	Pid	PV_WH_Lim	PV warning high limit	900.0	☐	0.0	☑	Archiving
3	LIC810	Pid	PV_TH_Lim	PV tolerance message high limit	850.0	☐	0.0	☑	No archiving
4	LIC810	Pid	PV_TL_Lim	PV tolerance message low limit	200.0	☐	0.0	☑	No archiving
5	LIC810	Pid	PV_WL_Lim	PV warning low limit	150.0	☐	0.0	☑	No archiving
6	LIC810	Pid	PV_AL_Lim	PV alarm low limit	100.0	☐	0.0	☑	Long-term archiving
7	LIC810	Pid	PV_Hyst	Hysteresis for PV alarms, warnings and tolerance messages	5.0	☐	0.0	☑	No archiving
8	LIC810	Pid	PV_A_DC	Delay time for incoming PV alarms [s]	0.0	☐	0.0	☐	
9	LIC810	Pid	PV_A_DG	Delay time for outgoing PV alarms [s]	0.0	☐	0.0	☐	
10	LIC810	Pid	PV_W_DC	Delay time for incoming PV warnings [s]	0.0	☐	0.0	☐	
11	LIC810	Pid	PV_W_DG	Delay time for outgoing PV warnings [s]	0.0	☐	0.0	☐	
12	LIC810	Pid	PV_T_DC	Delay time for incoming PV tolerance messages [s]	0.0	☐	0.0	☐	
13	LIC810	Pid	PV_T_DG	Delay time for outgoing PV tolerance messages [s]	0.0	☐	0.0	☐	
14	LIC810	Pid	PV_AH_En	1 = Enable PV alarm high	1	☐	0	☐	
15	LIC810	Pid	PV_WH_En	1 = Enable PV warning high	1	☐	0	☐	
16	LIC810	Pid	PV_TH_En	1 = Enable PV tolerance message high	0	☐	0	☐	

Figure 4 Spreadsheet-style interface for bulk transfer of alarm settings from the Master Alarm Database

Following the recommendations for alarm deadbands and on-off delays from the standard (shown in Table 2) can help prevent "nuisance" alarms during operation. A study by the ASM found that the use of on-off delays in combination with other configuration changes was able to reduce the alarm load on the operator by 45-90%.[4]

Signal Type	Deadband (Percent of Range)	Delay Time (On or Off)
Flow Rate	5%	15 seconds
Level	5%	60 seconds
Pressure	2%	15 seconds
Temperature	1%	60 seconds

Table 2. Recommended starting points for alarm deadbands and delay timers[3]

Note: Proper engineering judgement should be used when setting deadbands and delay times.

Configuration of alarm deadband (hysteresis), which is the change in signal from the alarm setpoint necessary to clear the alarm, can be optimized by a system that displays settings from multiple alarms at the same time, allowing them to be edited in bulk. This capability also makes it easy to review and update the settings after the system has been operating as recommended by the standard. Similar tools and procedures can be used to configure the on/off delay, which is the time that a process measurement remains in the alarm/normal state before the alarm is annunciated/cleared.

The design of the human machine interface (HMI) is critical for enabling the operator to ***detect, diagnose,*** and ***respond*** to an alarm within the appropriate timeframe. The proper use of color, text, and patterns directly affects the operator's performance. Since 8-12% of the male population is color blind, it is important to follow the design recommendations shown in Table 3 to ensure that changes in alarm state (normal, acknowledged, unacknowledged, suppressed) are easily detected.

Alarm State	Audible Indication	Visual Indications		
		Color	Symbol	Blinking
Normal	No	No	No	No
Unacknowledged (New) Alarm	Yes	Yes	Yes	Yes
Acknowledged Alarm	No	Yes	Yes	No
Return to Normal State Indication	No	Optional	Optional	Optional
Unacknowledged Latched Alarm	Yes	Yes	Yes	Yes
Acknowledged Latched Alarm	No	Yes	Yes	No
Shelved Alarm	No	Optional	Optional	No
Designed Suppression Alarm	No	Optional	Optional	No
Out of Service Alarm	No	Optional	Optional	No

Table 3 ISA-18.2 Recommended alarm state indications[3]

Symbols and faceplates provided with the system should comply with ISA-18.2's recommendations. Figure 5 shows an example where the unacknowledged alarm state can be clearly distinguished from the normal state by using both color (yellow box) and symbol (the letter "W"). This ensures that even a color blind operator can detect the alarm. The Out-of-Service state is also clearly indicated.

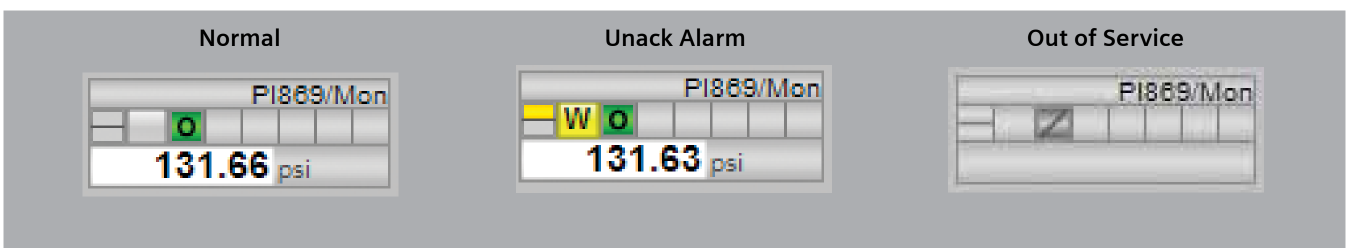


Figure 5 Alarm state indications in symbols

The standard recommends that the HMI should make it easy for the operator to navigate to the source of an alarm (single click) and provide powerful filtering capability within an alarm summary display.

Advanced alarming techniques can improve performance by ensuring that operators are presented with alarms only when they are relevant. Additional layers of logic, programming, or modeling are configured to modify alarm attributes or suppression state dynamically. One method described in ISA-18.2 is state-based alarming, wherein alarm attributes are modified based on the operating state of the plant or a piece of equipment.

State-based alarming can be applied to many situations. It can suppress a low flow alarm from the operator when it is caused by the trip of an associated pump. It can mask alarms coming from a unit or area that is shut down. In batch processes it can change which alarms are presented to the operator based on the phase (e.g. running, hold, abort) or based on the recipe.

One of the most challenging times for an operator is dealing with the flood of alarms that occur during a major plant upset. When a distillation column crashes, tens to hundreds of alarms may be generated. To help the operator respond quickly and correctly, the system should be able to hide all but the most significant alarms during the upset. For example, logic in the controller can determine the state of the column. The state parameter could then be used to determine which alarms should be presented to the operator based on a pre-configured state matrix, such as that shown in Figure 6.

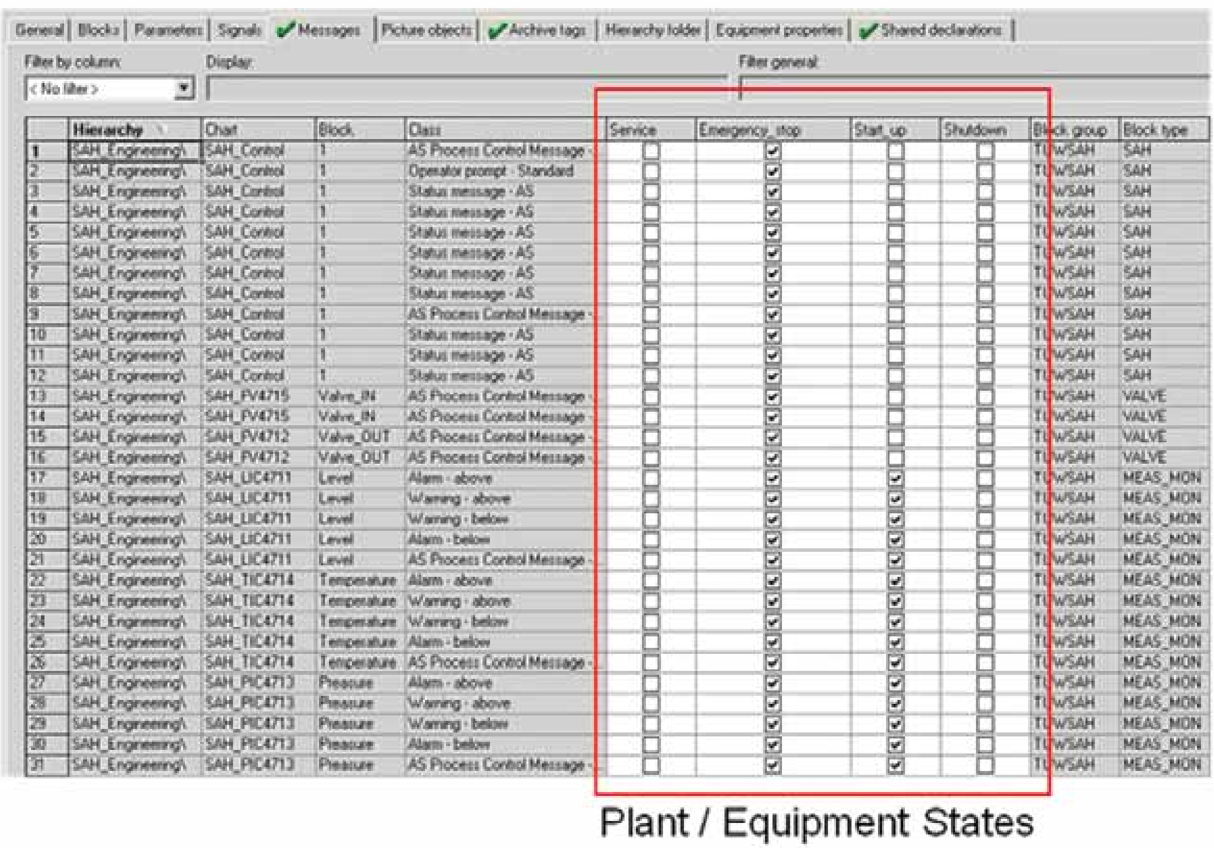


Figure 6 Configuration of state-based (advanced) alarming

4.4 Implementation (Phase E)

During the Implementation phase, the alarms in the control system are put into operation. Testing is a key activity, particularly as new instrumentation (and alarms) are added to the system over time or process designs changes are made. Equally important during this phase is training the operators of the system so they are comfortable with it, and so they trust it to help them do their job. The operators at the Milford Haven Refinery abandoned the system as "being more of a hindrance than a help" during the upset before the catastrophic explosion and fire.[5] Training the operators with process simulation tools can create a "drilled response" where corrective action is so well-reinforced that it is automatic.

4.5 Operation and maintenance (Phases F and G)

The standard defines the recommended tools for handling of alarms during operation. One of the most important is called alarm shelving, which is a tool for the operator to temporarily suppress an alarm, thus removing it from view. Shelving is critical for helping an operator respond effectively during a plant upset by manually hiding less important alarms. Alarms that are shelved will reappear after a preset time period so that they are not forgotten. When shelved an alarm should be removed from the active list and indication should be cleared from the HMI graphics and faceplates. Systems that support shelving must provide a display which lists all shelved alarms.

Figure 7 HMI list of shelved alarms

The standard also documents what should be included in an alarm response procedure. The information fleshed out during rationalization, such as an alarm's cause, potential consequence, corrective action, and the time to respond, should be made available to the operator. Ideally this information should be displayed online rather than in written form.

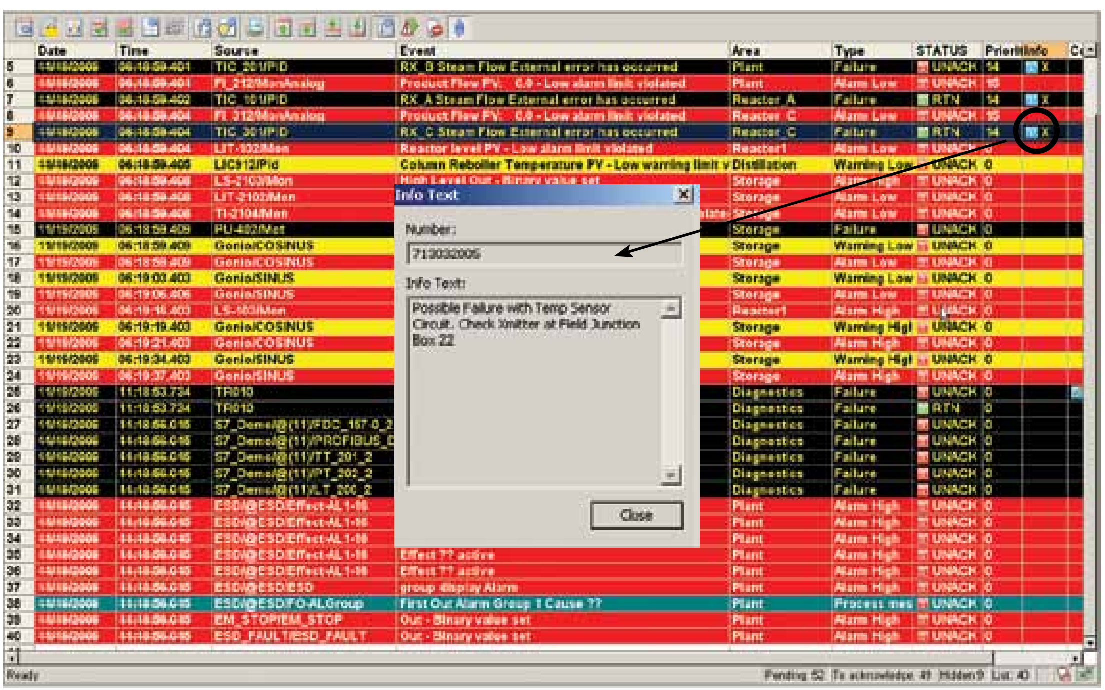


Figure 8 Display of alarm response information (derived during Rationalization phase)

Effective transfer of alarm status information between shifts is important in many facilities. The operator coming on shift in Texas City was provided with a three-line entry in the operator logbook, ill preparing him to address the situation leading up to the explosion. To improve shift transition, the system should allow operators to record comments for each alarm.

Maintenance is the stage where an alarm is taken out-of-service for repair, replacement, or testing. The standard describes the procedures that must be followed, including documenting why an alarm was removed from service, the details concerning interim alarms, special handling procedures, as well as what testing is required before it is put back into service. The standard requires that the system be able to show a complete list of alarms that are currently out-of-service. As a safety precaution, this list should be reviewed before putting a piece of equipment back into operation to ensure that all of the necessary alarms are operational.

The standard describes three possible methods for alarm suppression, which is any mechanism used to prevent the indication of the alarm to the operator when the base alarm condition is present. All three methods have a place in helping to optimize performance.

Suppression Method Per ISA-18.2	Definition	Relevant Phase
Shelving	A mechanism, typically initiated by the operator, to temporarily suppress an alarm	Operations
Suppressed by Design	Any mechanism within the alarm system that prevents the transmission of the alarm indication to the operator based on plant state or other conditions	Advanced Alarm Design
Out-of-Service	The state of an alarm during which the alarm indication is suppressed, typically manually, for reasons such as maintenance	Maintenance

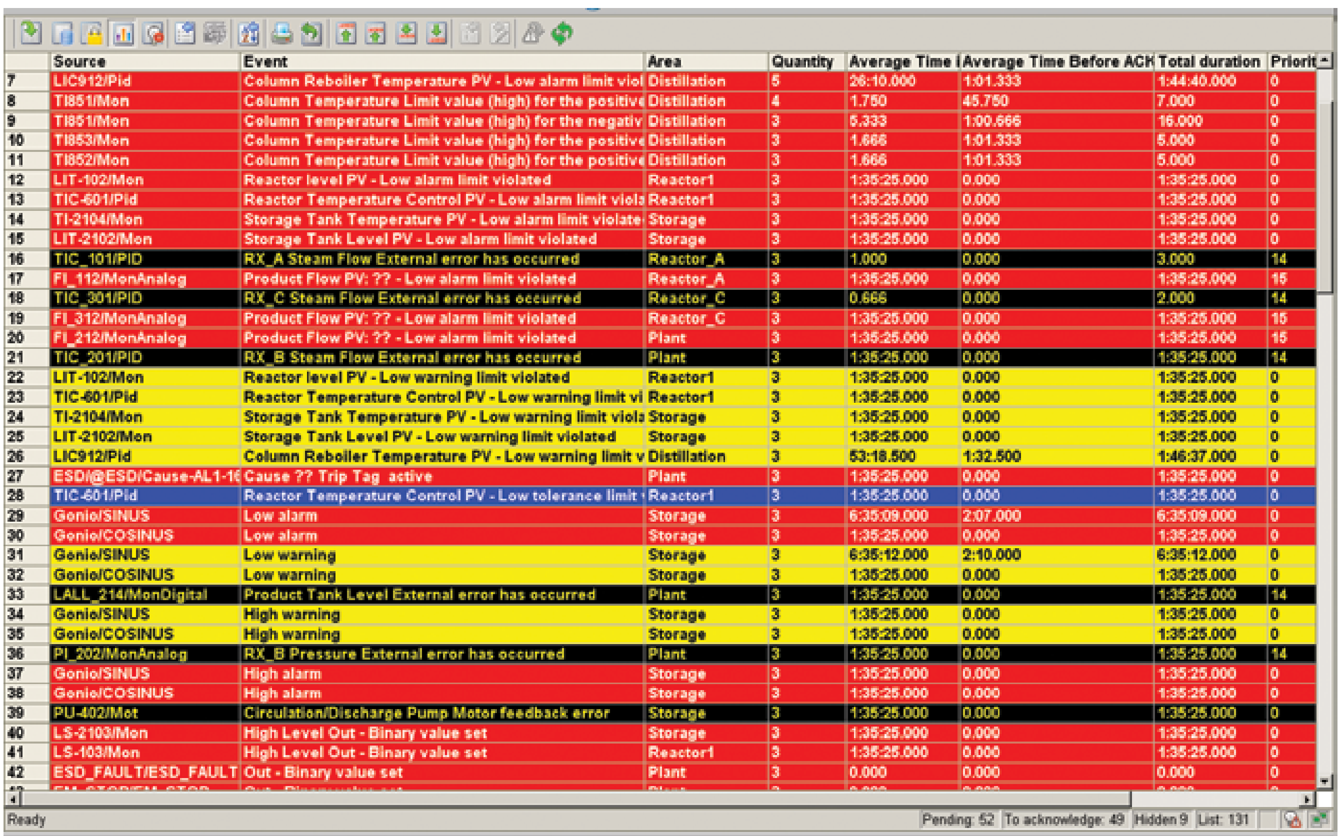
Table 4 – Methods for alarm suppression from ISA-18.2

4.6 Monitoring and assessment (Phase H)

The Monitoring and Assessment section of the standard describes how to analyze the performance of the alarm system against recommended key performance indicators (Table 5). One of the key metrics is the number of alarms that are presented to the operator. In order to provide adequate time to respond effectively, an operator should be presented with no more than one to two alarms every ten minutes. In many control rooms, operators are inundated with an average of one alarm every minute, which makes it challenging to respond correctly to each alarm. A related metric is the percentage of ten-minute intervals in which the operator received more than ten alarms, which indicates the presence of an alarm flood.

ISA-18.2 recommends using no more than three or four different alarm priorities in the system. To help operators know which alarms are most important so they can respond correctly, it is recommended that no more than 5% of the alarms be configured as high priority. The system should make it easy to review the configured alarm priority distribution, for example, by exporting alarm information to a .csv file for analysis in MS Excel.

Analysis should also include identifying nuisance alarms, which are alarms that annunciate excessively, unnecessarily, or do not return to normal after the correct response is taken (e.g., chattering, fleeting, or stale alarms). The system should have the capability of calculating and displaying statistics, such as alarm frequency, average time in alarm, time between alarms, and time before acknowledgement. It is not uncommon for the majority of alarms (up to 80%) to originate from a small number of tags (10 – 20). This frequency analysis makes it easy to identify these "bad actors" and fix them. The "average time in alarm" metric can help identify chattering alarms, which are alarms that repeatedly transition between the alarm state and the normal state in a short period of time.



	Source	Event	Area	Quantity	Average Time i	Average Time Before ACK	Total duration	Priorit
7	LIC912/Pid	Column Reboiler Temperature PV - Low alarm limit viol	Distillation	5	26:10.000	1:01.333	1:44:40.000	0
8	TI851/Mon	Column Temperature Limit value (high) for the positive	Distillation	4	1.750	45.750	7.000	0
9	TI851/Mon	Column Temperature Limit value (high) for the negativ	Distillation	3	5.333	1:00.666	16.000	0
10	TI853/Mon	Column Temperature Limit value (high) for the positive	Distillation	3	1.666	1:01.333	5.000	0
11	TI852/Mon	Column Temperature Limit value (high) for the positive	Distillation	3	1.666	1:01.333	5.000	0
12	LIT-102/Mon	Reactor level PV - Low alarm limit violated	Reactor1	3	1:35:25.000	0.000	1:35:25.000	0
13	TIC-601/Pid	Reactor Temperature Control PV - Low alarm limit viola	Reactor1	3	1:35:25.000	0.000	1:35:25.000	0
14	TI-2104/Mon	Storage Tank Temperature PV - Low alarm limit violate	Storage	3	1:35:25.000	0.000	1:35:25.000	0
15	LIT-2102/Mon	Storage Tank Level PV - Low alarm limit violated	Storage	3	1:35:25.000	0.000	1:35:25.000	0
16	TIC_101/PID	RX_A Steam Flow External error has occurred	Reactor_A	3	1.000	0.000	3.000	14
17	FI_112/MonAnalog	Product Flow PV: ?? - Low alarm limit violated	Reactor_A	3	1:35:25.000	0.000	1:35:25.000	15
18	TIC_301/PID	RX_C Steam Flow External error has occurred	Reactor_C	3	0.666	0.000	2.000	14
19	FI_312/MonAnalog	Product Flow PV: ?? - Low alarm limit violated	Reactor_C	3	1:35:25.000	0.000	1:35:25.000	15
20	FI_212/MonAnalog	Product Flow PV: ?? - Low alarm limit violated	Plant	3	1:35:25.000	0.000	1:35:25.000	15
21	TIC_201/PID	RX_B Steam Flow External error has occurred	Plant	3	1:35:25.000	0.000	1:35:25.000	14
22	LIT-102/Mon	Reactor level PV - Low warning limit violated	Reactor1	3	1:35:25.000	0.000	1:35:25.000	0
23	TIC-601/Pid	Reactor Temperature Control PV - Low warning limit vi	Reactor1	3	1:35:25.000	0.000	1:35:25.000	0
24	TI-2104/Mon	Storage Tank Temperature PV - Low warning limit viola	Storage	3	1:35:25.000	0.000	1:35:25.000	0
25	LIT-2102/Mon	Storage Tank Level PV - Low warning limit violated	Storage	3	1:35:25.000	0.000	1:35:25.000	0
26	LIC912/Pid	Column Reboiler Temperature PV - Low warning limit v	Distillation	3	53:18.500	1:32.500	1:46:37.000	0
27	ESD/@ESD/Cause-AL1-1€	Cause ?? Trip Tag active	Plant	3	1:35:25.000	0.000	1:35:25.000	0
28	TIC-601/Pid	Reactor Temperature Control PV - Low tolerance limit	Reactor1	3	1:35:25.000	0.000	1:35:25.000	0
29	Gonio/SINUS	Low alarm	Storage	3	6:35:09.000	2:07.000	6:35:09.000	0
30	Gonio/COSINUS	Low alarm	Storage	3	1:35:25.000	0.000	1:35:25.000	0
31	Gonio/SINUS	Low warning	Storage	3	6:35:12.000	2:10.000	6:35:12.000	0
32	Gonio/COSINUS	Low warning	Storage	3	1:35:25.000	0.000	1:35:25.000	0
33	LALL_214/MonDigital	Product Tank Level External error has occurred	Plant	3	1:35:25.000	0.000	1:35:25.000	14
34	Gonio/SINUS	High warning	Storage	3	1:35:25.000	0.000	1:35:25.000	0
35	Gonio/COSINUS	High warning	Storage	3	1:35:25.000	0.000	1:35:25.000	0
36	PI_202/MonAnalog	RX_B Pressure External error has occurred	Plant	3	1:35:25.000	0.000	1:35:25.000	14
37	Gonio/SINUS	High alarm	Storage	3	1:35:25.000	0.000	1:35:25.000	0
38	Gonio/COSINUS	High alarm	Storage	3	1:35:25.000	0.000	1:35:25.000	0
39	PU-402/Mot	Circulation/Discharge Pump Motor feedback error	Storage	3	1:35:25.000	0.000	1:35:25.000	0
40	LS-2103/Mon	High Level Out - Binary value set	Storage	3	1:35:25.000	0.000	1:35:25.000	0
41	LS-103/Mon	High Level Out - Binary value set	Reactor1	3	1:35:25.000	0.000	1:35:25.000	0
42	ESD_FAULT/ESD_FAULT	Out - Binary value set	Plant	3	0.000	0.000	0.000	0

Ready | Pending: 52 | To acknowledge: 49 | Hidden 9 | List: 131

Figure 9 Pinpointing nuisance alarms from an alarm frequency display in the HMI

Another key objective of the Monitoring & Assessment phase is to identify stale alarms, which are those alarms that remain in the alarm state for an extended period of time (> 24 hours). The system should allow the alarm display to be filtered, based on time in alarm, in order to create a stale alarm list. Alarm display filters should be savable and reusable so that on-demand reports can be easily created. All information contained in the alarm display should be exportable for ad-hoc analysis.

Alarm Performance Metrics Based Upon at Least 30 Days of Data		
Metric	**Target Value**	
Annunciated Alarms per time	Target Value: Very likely to be acceptable	Target value: Maximum manageable
Annunciated Alarms per day per operating position	150 alarms per day	300 alarms per day
Annunciated alarms per hour per operating position	6 (average)	12 (average)
Annunciated alarms per 10 minutes per operating position	1 (average)	2 (average
Metric	**Target Value**	
Percentage of hours containing more than 30 alarms	<1%	
Percentage of 10-minute periods containing more than 10 alarms	<1%	
Maximum number of alarms in a 10-minute 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% to 5% maximum, with action plans to address deficiencies	
Quantity of chattering and fleeting alarms	Zero, develop action plans to correct any that occur	
Stale alarms	<5/day, with action plans to address	
Annunciated priority distribution	If using three priorities: 80% low, 15% medium, 5% high If using four priorities: 80% low, 15% medium, 5% high, <1% "highest" Other special-purpose priorities are excluded from the calculation	
Unauthorized alarm suppression	Zero alarms suppressed outside of controlled or approved methodologies	
Unauthorized alarm attribute changes	Zero alarm attribute changes outside of approved methodologies or Management of Change (MOC)	

Table 5 ISA-18.2 Alarm Performance Metrics[3]

4.7 Management of change (Phase I)

Even the most well-designed alarm system may not prevent problems if there is not strict control over access to configuration changes. Management of change entails the use of tools and procedures to ensure that modifications to the alarm system (such as changing an alarm's limit) get reviewed and approved prior to implementation. Once the change is approved, the Master Alarm Database should be updated to keep it current.

All changes made through the HMI should be automatically recorded with the date / time stamp, "from" and "to" values, along with who made the change. The system should provide the capability to set up access privileges (such as who can acknowledge alarms, modify limits, or disable alarms) on an individual and a group basis. It is also important to prevent unauthorized configuration changes from the engineering station.

It is good practice to periodically compare the actual running alarm system configuration to the Master Alarm Database to ensure that no unauthorized configuration changes have been made. The system should provide tools to facilitate this comparison in order to make it easy to discover differences (e.g. alarm limit has been changed from 10.0 to 99.99). These differences can then be corrected to ensure consistency and traceability.

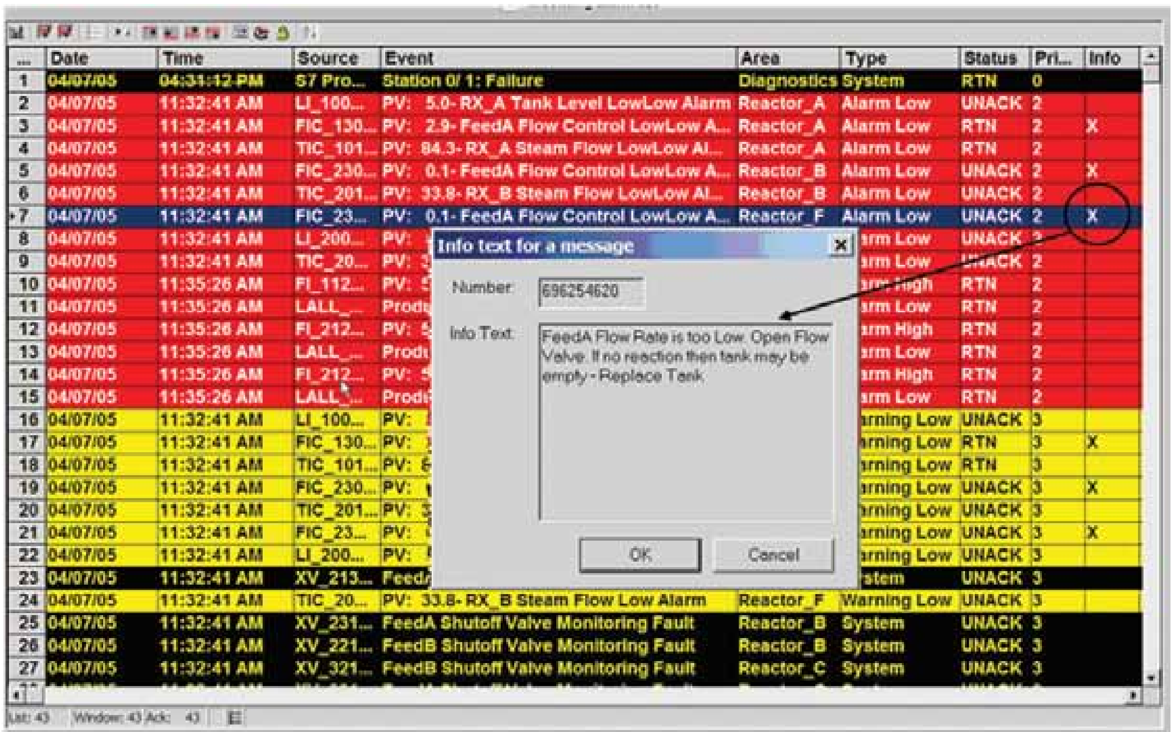


Figure 10 Tools for comparing the online system to the Master Alarm Database

4.8 Audit (Phase J)

The last phase in the alarm management life-cycle is Audit. During this phase, periodic reviews are conducted of the alarm management processes that are used in the plant. The operation and performance of the system is compared against the principles and benchmarks documented in the alarm philosophy. The goal is to maintain the integrity of the alarm system and to identify areas of improvement. The alarm philosophy document is modified to reflect any changes resulting from the audit process.

5.0 Getting started

No matter whether you are working with an installed system, are looking to migrate, or are putting in a new system, the ISA-18.2 standard provides a useful framework for improving your alarm management practices. There is no "right" or "wrong" place to start; however, your system will likely dictate which phase of the alarm management life-cycle to focus on first. Alarm philosophy is a good place to start for a new system, while monitoring and assessment can be ideal for an existing system. Here are some of the key actions on which to concentrate when starting to adopt ISA-18.2.

1) Develop an alarm philosophy document to establish the standards for how your organization will do alarm management.
2) Rationalize the alarms in the system to ensure that every alarm is necessary, has a purpose, and follows the cardinal rule – that it requires an operator response.
3) Analyze and benchmark the performance of the system and compare it to the recommended metrics in ISA-18.2. Start by identifying nuisance alarms, which can be addressed quickly and easily – this rapid return on investment may help justify additional investment in other alarm management activities.
4) Implement Management of Change. Review access privileges and install tools to facilitate periodic comparisons of the actual configuration vs. to the Master Alarm Database.
5) Audit the performance of the alarm system. Talk with the operators about how well the system supports them. Do they know what to do in the event of an alarm? Are they able to quickly diagnose the problem and determine the corrective action? Also, analyze their ability to detect, diagnose, and respond correctly and in time.
6) Perform a gap analysis on your legacy control system. Identify gaps compared to the standard (e.g. lack of analysis tools) and opportunities for improvement. Consider the cost vs. benefit of upgrading your system to improve its performance and for compliance with ISA-18.2. In many cases a modern HMI can be added on top of a legacy control system to provide enhanced alarm management capability without replacing the controller and I/O.

6.0 Conclusion

Following the ISA-18.2 standard will become increasingly important as it is adopted by industry, insurance, and regulatory bodies. The standard includes recommendations and requirements that can stop poor alarm management, which acts as a barrier to operational excellence. Look for a system that provides a comprehensive set of tools that can help you to follow the alarm management lifecycle and address the most common alarm issues – leading to a safer and more efficient plant.

Depending upon the capabilities of the native control system, additional third-party tools may be required to deliver the benefits of ISA-18.2. Finding a control system which provides, out-of-the-box, the capabilities demanded by the standard can reduce life-cycle costs and make it easier for personnel to support and maintain. A checklist of the most important alarm management capabilities for compliance with ISA-18.2 is provided in Appendix A.

For more information, go the ISA website *www.isa.org* to get a copy of the standard (free to all ISA members).

7.0 References

1. "The Buncefield Investigation" - www.buncefieldinvestigation.gov.uk/reports/index.htm
2. "BP America Refinery Explosion" U.S. CHEMICAL SAFETY BOARD www.chemsafety.gov/investigations
3. ANSI/ISA-18.2-2009 "Management of Alarm Systems for the Process Industries". www.isa.org
4. Zapata, R. and Andow, P., "Reducing the Severity of Alarm Floods", www.controlglobal.com
5. "The Explosion and Fires at the Texaco Refinery, Milford Haven, 24 July 1994", HSE Books, Sudbury, U.K. (1995).
6. EEMUA 191 (2007), "Alarm Systems: A Guide to Design, Management and Procurement Edition 2". The Engineering Equipment and Materials Users Association. www.eemua.co.uk
7. Abnormal Situation Management Consortium, www.asmconsortium.net
8. NAMUR (Interessengemeinschaft Automatisierungstechnik der Prozessindustrie), www.namur.de
9. Podcast: "Saved by the Bell: A look at ISA's New Standard on Alarm Management", www.controlglobal.com/multimedia/2009/AlarmMgmtISA0907.html

Features and requirements

Feature	System Recommendation/Requirements	Reason/Purpose
Alarm rationalization results documentation	Provide ability to document alarm consequence, cause, and recommended action within control system configuration	Information derived from the Rationalization phase can help operators diagnose and respond quickly and accurately
Alarm response procedures documentation	Provide ability to display alarm consequence, cause, and recommended action to operator from the HMI	Information derived from the Rationalization phase can help operators diagnose and respond quickly and accurately
Nuisance alarm minimization settings	Provide both alarm deadband and on/off delay parameters for each alarm	Allows analysis and review of alarm limits, deadband, and on-off delays to prevent nuisance alarms
Bulk alarm configuration and analysis capability	Provide ability to view and edit alarm attributes (e.g. limits, priority, deadband, on-off delay) from multiple alarms simultaneously in a spreadsheet-style interface	Allows analysis and review of alarm limits, deadband, and on-off delays to prevent nuisance alarms
Alarm priority distribution analysis	Provide tools to make it easy to review configured alarm priority distribution	For verification that distribution follows recommendations of ISA-18.2 so that operators are not presented with too many "high" priority alarms
HMI symbol design	Default HMI symbols and faceplates should comply with ISA-18.2's design recommendations regarding use of sound, color, symbol, and blinking	Helps operators (even those that are color-blind) to be able to quickly detect an alarm
Highly managed alarms visualization	Provide dedicated displays and icons within the HMI for representing status of "highly managed alarms" (e.g. safety alarms)	Separates alarm information to ensure that operators can always see the status of highly managed alarms
Advanced alarming capability	Support common techniques for advanced alarming, including first-out alarming and state-based alarming	In many cases simply following the guidelines for basic alarm design is not sufficient to achieve required performance
Alarm shelving capability	Provide capability for operator to shelve individual alarms and view a list of all shelved alarms	Helps operators to respond to plant upsets by allowing them to temporarily suppress alarms that are not significant
Operator comments capability	Provide ability for operator to add comments to individual alarm events	Enables documentation of operator response, device status, and flagging of alarms for maintenance and/or improvement
Out-of-service alarms capability and tracking	Provide capability for taking alarms out of service and for viewing a list of all such alarms	Ensures that alarms that are taken out of service for maintenance are clearly visible; the list should be reviewed before starting any equipment.
Alarm suppression capability	Support ability to suppress alarms based on operating conditions or plant states	Allows alarms to be suppressed based on the state of equipment (e.g. non-operational) or the phase of a batch process
Alarm flood suppression capability	Support ability to automatically suppress insignificant alarms during a flood and display only the most relevant alarms to the operator	Helps reduce the severity of alarm floods or prevent them altogether so that the operator can respond more effectively during a process upset
Nuisance alarms identification	Provide analysis tools which calculate and display alarm frequency, average time in alarm, time between alarms, and time before acknowledgement	Helps identify common nuisance alarms (e.g. chattering alarms, fleetings alarms, stale alarms) so that they can be fixed
Operator alarm load analysis	Provide analysis tools that calculate the number of alarms presented to the operator per time period (e.g. quantity of alarms/10 minutes)	Helps benchmark operator alarm loading to ensure that operators are not being presented with too many alarms to respond effectively
Online filtering capability and on-demand reports creation	Alarm display filters should be savable and reusable so that on-demand "reports" can be created easily. All information contained in the alarm display should be exportable for analysis	Minimizes the effort and makes it easy to view and analyze alarm system performance
Management of change tools	The system should provide tools to allow direct comparison between alarm settings in the Master Alarm Database and in the running system	Detect changes in alarm settings so that a change request can be initiated or restored to the value established during rationalization

Siemens Industry, Inc.
3333 Old Milton Parkway
Alpharetta, GA 30005
1-800-964-4114

info.us@siemens.com

www.usa.siemens.com/process

Subject to change without prior notice
Order No.: PAWP-00020-0110