PROCESS AUTOMATION

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

SIEMENS

Contents

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 increasing adoption of the ISA standard on alarm management. The ISA-18.2 standard, which provides a blueprint for creating a safer and more productive plant, has been adopted by OSHA and insurance agencies as "good engineering practice." This white paper provides an overview of the standard and examples of how to follow it. It also describes the most important capabilities 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.

1.0

Introduction: Why alarm management is important

In an increasingly competitive environment, manufacturers in the process industries are focusing on operational excellence as a key to short-term survival and 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 24/7. It also impacts the safety of a plant and its personnel, having played a major part in the accidents at Three Mile Island in Pennsylvania, the Texas City Refinery in Texas, and the Milford Haven Refinery and Buncefield Oil Depot in the United Kingdom – all of which resulted in significant injuries, loss of life and fines as well as damage to equipment, property, and 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 notified the operators of the unsafe and abnormal conditions that existed within the tower and blowdown drum.[2]

The standard ANSI/ISA-18.2, "Management of Alarm Systems for the Process Industries," and its sister document IEC 62682 define the recommended and required practices for effective alarm management. 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 (Abnormal Situation Management Consortium). Alarm management is not a "once and done" activity; rather, it is a process requiring 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 has become "recognized and generally accepted good engineering practice" (RAGAGEP) by both insurance companies and regulatory agencies. As such, it becomes the expected minimum practice.
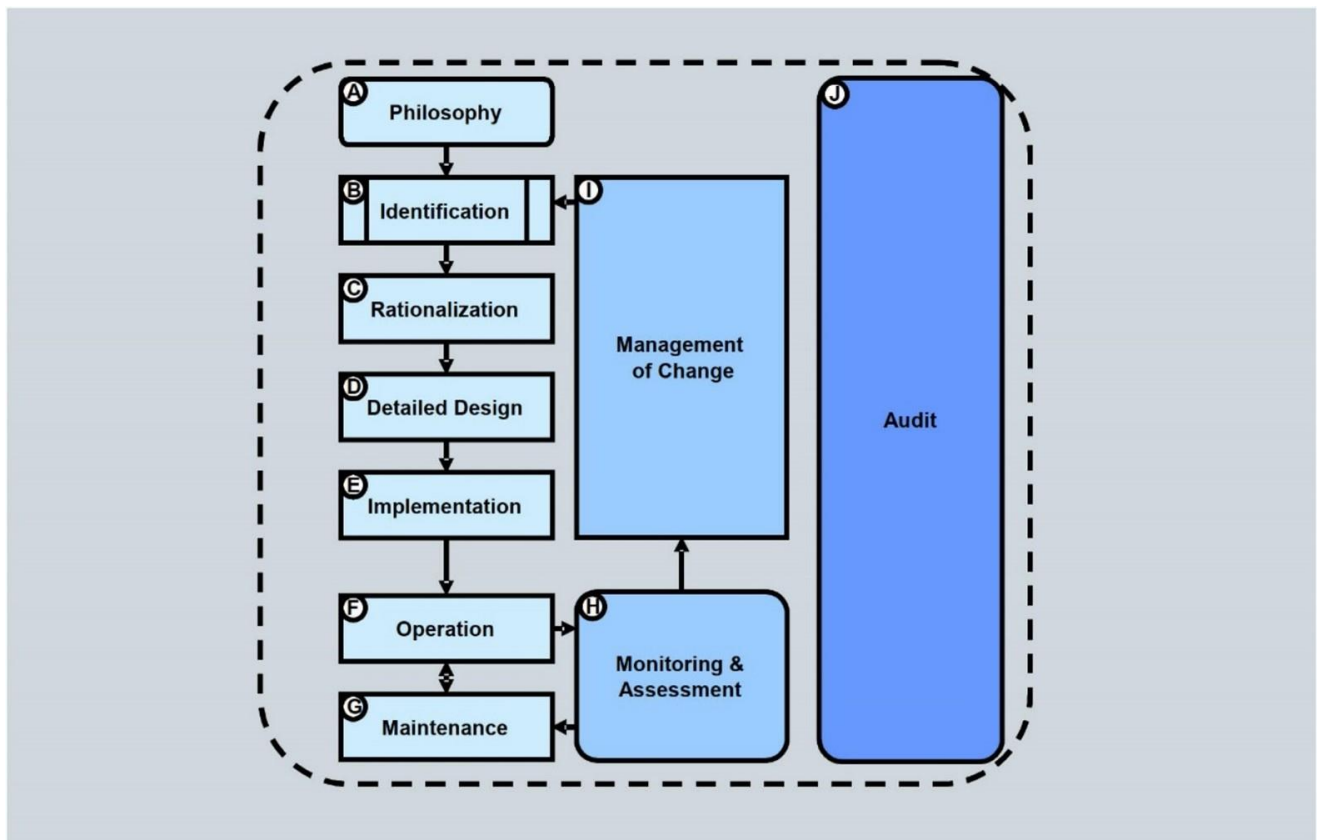

Figure 1 – Alarm management life cycle[3]

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 timely response.

Figure 2 – Definition of "alarm" from ISA-18.2[3]

One of the most important principles of alarm management is that an alarm requires a response. This means that if the operator does not need to respond to an alarm (because unacceptable consequences would not occur), then the alarm should not be configured. 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 ignored by the operator	"Nuisance" alarms (chattering alarms and fleeting alarms), faulty hardware, redundant alarms, cascading alarms, incorrect alarm settings, alarms that have not been rationalized
When alarms occur, operators do not know how to respond	Lack of training and insufficient alarm response procedures (Alarm Help)
Minor plant upsets generate many alarms	Average alarm load is too high, redundant alarms, cascading alarms, alarms that 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 that 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, alarm limit is dependent on operating state
During an upset, operators are flooded with so many alarms that they do not know which ones to respond to first	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 indicators, 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 to prevent a defined consequence?
- 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 – alarms classified as critical to process safety for the protection of human life or the environment – are also important to identify. These alarms warrant special treatment when it comes to training, testing, and HMI display in order to achieve maximum reliability.

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 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 can be made available to the operator online through the HMI.

Figure 3 – Entering cause-corrective action information from rationalization directly into the DCS

One major benefit of conducting a rationalization is determining the minimum set of alarms needed to keep the process safe and under control. Too many projects follow an approach in which the practitioner enables all alarms provided by the DCS, whether or not they are needed, 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 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 toward eliminating these 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 remainder of the alarm design is completed and information contained in the Master Alarm Database (such as alarm limit and priority) is used to configure the control 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.

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 (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 judgment should always be used when setting deadbands and delay timers.

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. Such features are provided, for example, by the SIMATIC PCS 7 Advanced Process Library. User-configurable message classes allow alarms to be prioritized based on criteria such as the potential consequence and operator response time, ensuring that the alarm's relative importance carries through consistently in its presentation throughout the operating system.

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 colorblind, 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	Color	Symbol	Blinking
Normal	No	No	No	No
Unacknowledged (new) alarm	Yes	Yes	Yes	Yes
Acknowledged alarm	No	Yes	Yes	No
Return-to-normal, unacknowledged alarm	No	Combination	Combination	Optional
Shelved alarm	No	Optional	Optional	No
Suppressed-by-design 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 colorblind operator can detect the alarm. The out-of-service state is also clearly indicated.

Normal   **Unacknowledged alarm**   **Out-of-service alarm**

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 on the recipe.

One of the most significant challenges for an operator is dealing with the flood of alarms resulting from 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 design changes are made. Equally important during this phase is training the operators of the system so they are comfortable with it and 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 to help an operator manage nuisance alarms so that they are not a distraction. Alarms that are shelved will reappear after a preset time period to ensure 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 listing all shelved alarms.

For example, Version 9.1 of the Siemens distributed control system SIMATIC PCS 7 provides two features to optimize the alarm shelving process. A dialog option allows the operator to input a reason for manually suppressing an alarm, which conforms with IEC 62682 requirements for alarm traceability. Additionally, the display of shelved alarms is provided via an icon that becomes active only when such alarms exist. Clicking the icon opens a comprehensive overview window that shows the quantity of suppressed alarms and links to more details about each suppressed alarm, simplifying operator access to the relevant alarm list.
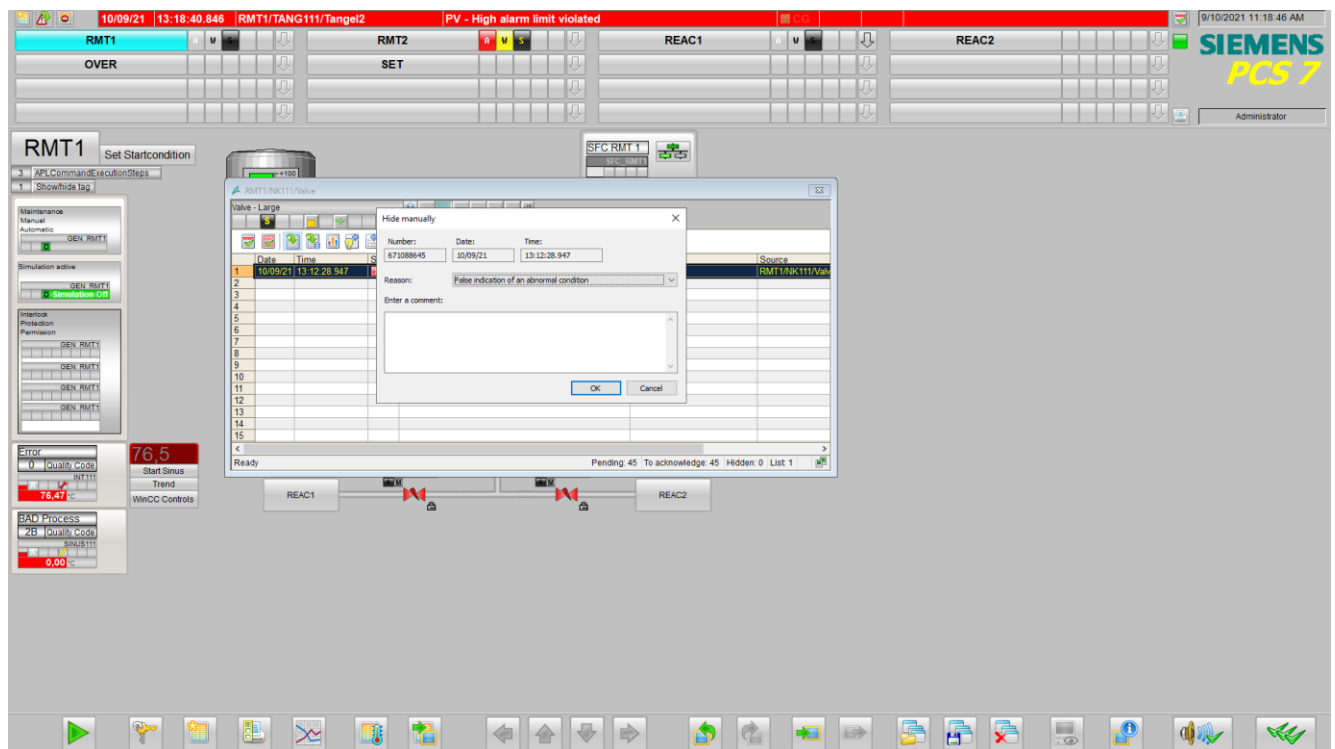
Figure 7 – Manual alarm suppression dialog box

Figure 8 – Active icon indicating that hidden alarms exist (circled in red)

Figure 9 – 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.

From an operations point of view, the ability to display an alarm response procedure in context from within the operating system is a gamechanger in the quest to better manage abnormal situations. An alarm response procedure known as "Alarm Help" in SIMATIC PCS 7 provides the operator with relevant guidance on each alarm. It is meant to help improve the operator's response to an alarm by reducing the time it takes to correctly diagnose the problem and determine the appropriate corrective action. This is especially crucial for safety-critical alarms or alarms that do not occur very often in order to prevent human error.

The information for Alarm Help is typically captured during rationalization in the Master Alarm Database. Some third-party tools (such as exida's SILAlarm™) support import of the rationalization results directly into PCS 7 Process Object View, a Microsoft Excel-like tool, thus automatically configuring Alarm Help for each rationalized alarm. The alarm rationalization process leverages the experience of a plant's most senior operators. Because Alarm Help displays this information, everyone in the plant – including new operators – gets to see what the most knowledgeable operators would do in response to an alarm. This leads to quick, consistent responses that more effectively prevent plant upsets from becoming costly incidents.
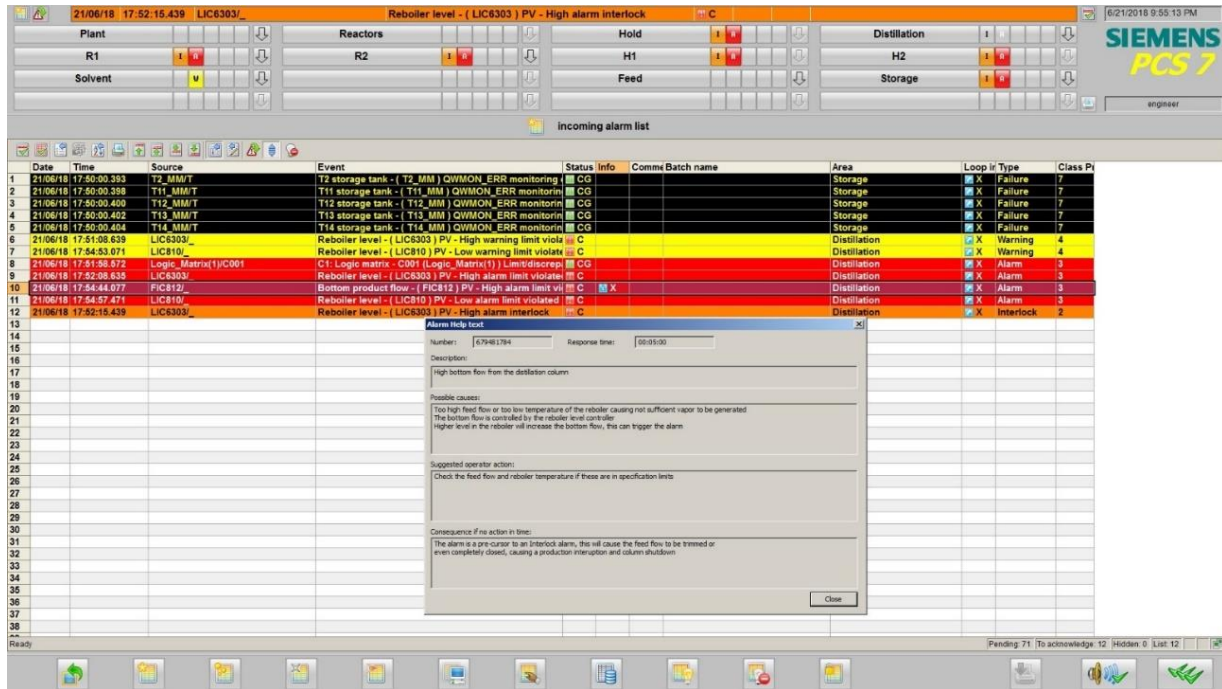
Figure 10 – The Alarm Help procedure provides operators with relevant guidance on each alarm

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 or require operators to record comments for each alarm. With SIMATIC PCS 7 Version 9.1, it is possible to configure whether a comment must be entered before an operator can acknowledge an alarm. Comments inputted in response to alarms cannot be overwritten; instead, new comments must be added underneath those that already exist, thereby ensuring a continual log of actions taken. This reduces risk following shift changes and ensures that acknowledgment of critical messages can be easily traced.
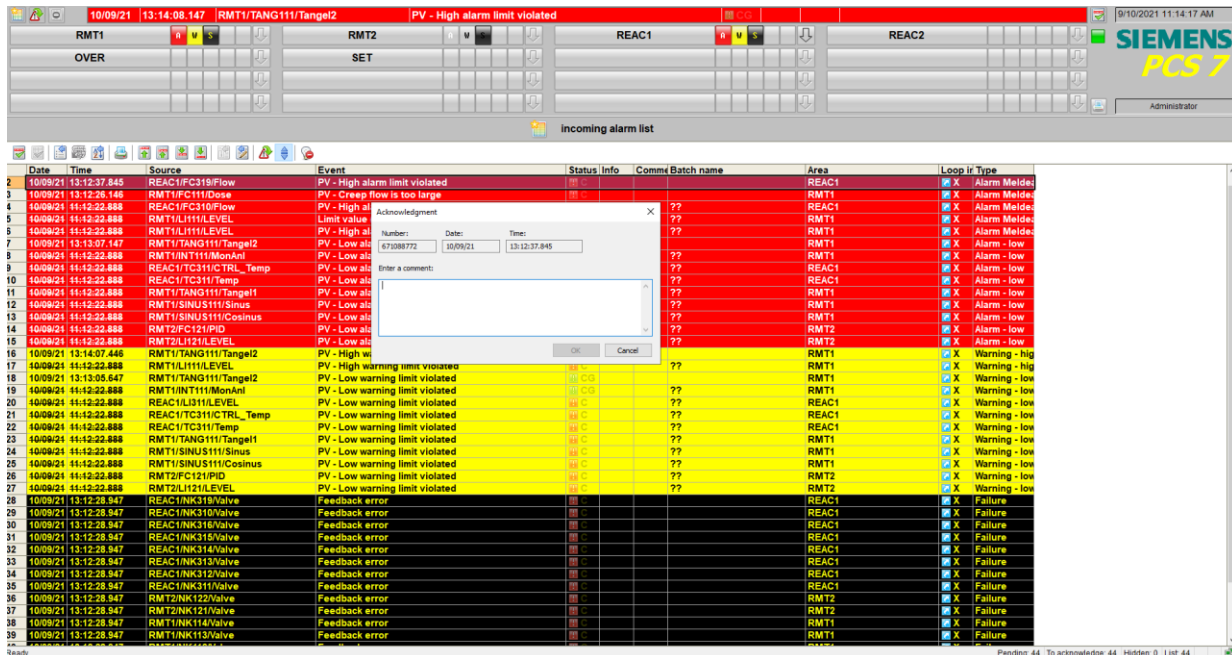
Figure 11 – Inputting a comment in order to be allowed to acknowledge an alarm

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, and which 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 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 with engineering controls (e.g., time-limited) that un-suppress the alarm	Operation
Suppressed by design	Any mechanism within the alarm system that prevents the annunciation of the alarm to the operator based on plant state or other conditions	Detailed 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[3]

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 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.

To help operators know which alarms are most important so they can respond correctly, the system should allow for user-defined sorting of alarm lists to ensure the site-specific alarm philosophy is properly executed. For example, SIMATIC PCS 7 Version 9.1 allows the operator to sort alarms using several criteria – including priority, alarm state and time – in either ascending or descending order. ISA-18.2 recommends using no more than three or four different alarm priorities in the system, and 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 (e.g., by exporting alarm information to a .csv file for analysis in Microsoft 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 acknowledgment. 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. Chattering alarms are a major source of nuisance alarms and should be eliminated.
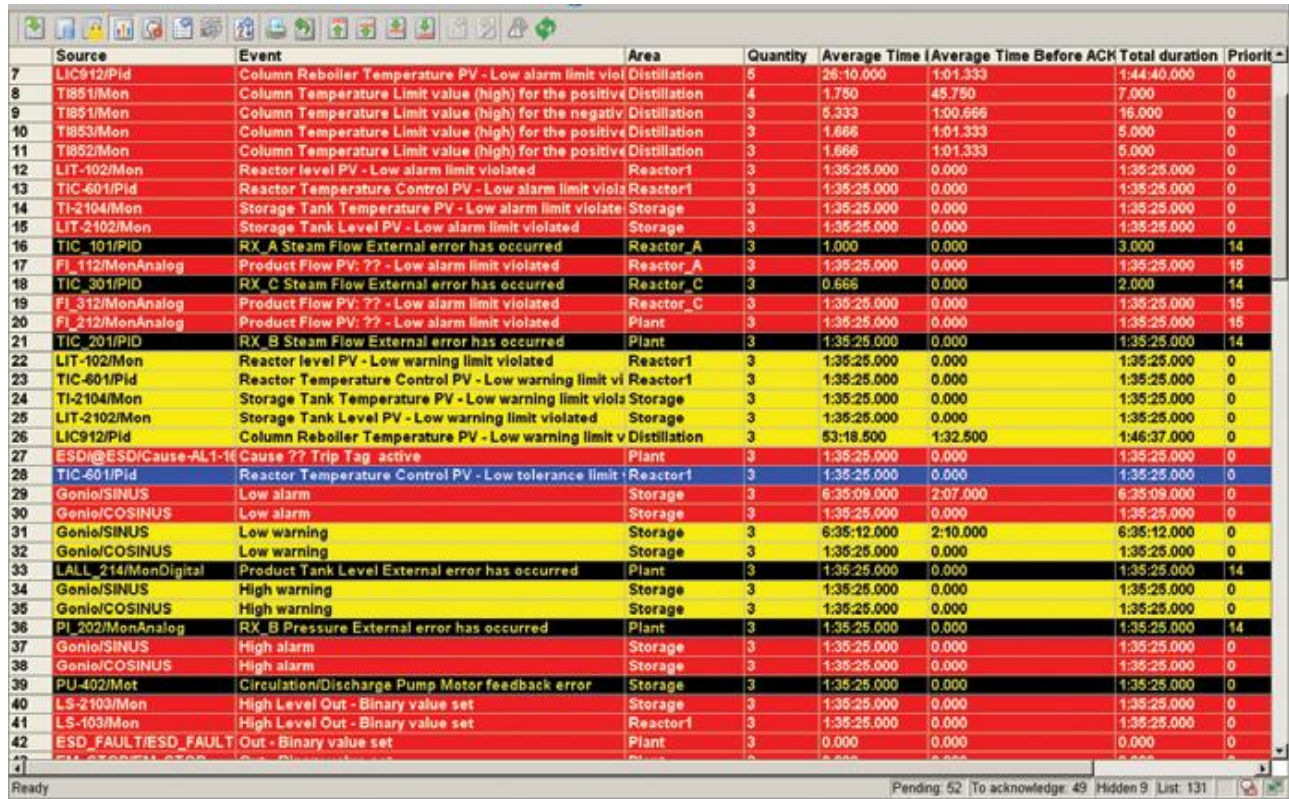
Figure 12 – Pinpointing nuisance alarms from an alarm frequency display in the HMI

Metric	Target value
Annunciated alarms per hour per operating position	Very likely to be acceptable: 6 (average) Maximum manageable: 12 (average)
Annunciated alarms per 10 minutes per operating position	Very likely to be acceptable: 1 (average) Maximum manageable: 2 (average)
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
Quantity of chattering and fleeting alarms	Zero, with 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

Table 5 – ISA-18.2 alarm performance metrics based upon at least 30 days of data[3]

Another key objective of the Monitoring and 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.

4.7 Management of change (Phase I)

Even the most well-designed alarm system may not prevent problems without 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) go through a thorough review and authorization process prior to implementation. An example of this standard in action can be found in SIMATIC PCS 7 Version 9.1, where message filters include the option to set which level of authorization a user must have in order to configure or modify the filter.

All changes made through the HMI should be automatically recorded with the date/time stamp, "from" and "to" values, and 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.

Once a change is approved, the Master Alarm Database should be updated to keep it current. 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. if an alarm limit has been changed from 10.0 to 99.99). These differences can then be corrected to ensure alarm system integrity.

4.8 Audit

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 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, looking to migrate, 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 of requiring 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. 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 further 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 with a comprehensive set of tools that can help you to follow the alarm management life cycle 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 that provides the capabilities demanded by the standard, right out of the box, 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 and to get a copy of the standard (free to all ISA members), visit the ISA website: www.isa.org

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) "Saved by the Bell: A Look at ISA's New Standard on Alarm Management," Podcast, www.controlglobal.com/multimedia/2009/AlarmMgmtISA0907.html

APPENDIX A

Important alarm management capabilities for compliance with ISA-18.2

Feature	System recommendation/ requirements	Reason/purpose
Alarm rationalization results documentation	Provide the ability to document alarm consequence, cause, and recommended action within the control system configuration	Information derived from the Rationalization phase can help operators diagnose and respond quickly and accurately
Alarm response procedures documentation	Provide the ability to display alarm consequence, cause, and recommended action to operators 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 the 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 ISA-18.2 recommendations 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 colorblind) 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 and state-based alarming	In many cases, simply following the guidelines for basic alarm design is not sufficient to achieve the required performance
Alarm shelving capability	Provide the capability for the operator to shelve individual alarms and view a list of all shelved alarms	Helps operators respond to plant upsets by allowing them to temporarily suppress alarms that are not significant
Operator comments capability	Provide the ability for operators 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	Support the 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 suppression capability	Support the 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 the 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 that 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, fleeting 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