Economic and Effective Alarm Management

LISTEN.
THINK.
SOLVE.®

Allen-Bradley • Rockwell Software

Rockwell Automation

Introduction

Like many industrial process plants, your manufacturing facility's distributed control system (DCS) may have a poorly functioning alarm system. Formal alarm management, which includes effective design, implementation, and maintenance, offers a solution. But limited funding and/or resources often present a barrier to adoption. This white paper – the first in a three part series – examines the ANSI/ISA 18.2 Standard: Management of Alarm Systems for the Process Industries and focuses on the Monitoring & Assessment entry point to alarm management.

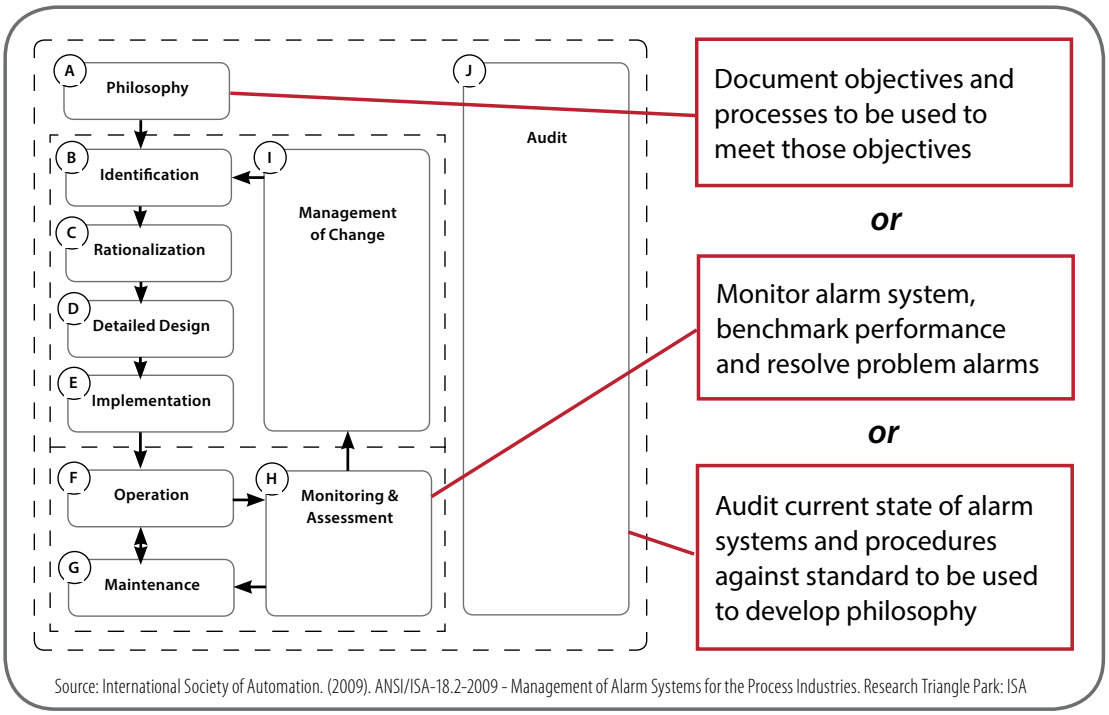


Figure 1 illustrates the 18.2 alarm management lifecycle, including three entry points. For new alarm system projects, the starting point is always the Philosophy stage. For existing systems, however, it is expedient, effective, and economical to begin with Monitoring & Assessment. The Audit is the third entry point.

This three-part white paper series will cover these areas in the 18.2 lifecycle stages:

1. **Monitoring & Assessment** – A limited, but effective, program of nuisance/bad actor alarm elimination.

2. **Performance Benchmarking and Philosophy** – Benchmarking includes alarm analysis, operator analysis, and gap analysis. The Philosophy stage results in a document that details the recommended approach to how a company addresses alarm management through all stages of the lifecycle.

3. **Rationalization and Implementation** – Rationalization is the process of reviewing and justifying alarms that meet criteria that are established in the Philosophy Document. Implementation includes all infrastructure changes to support a new alarm system or modifications to an existing alarm system.

For immediate alarm reduction, Monitoring & Assessment is an excellent entry point into ANSI/ISA 18.2. This first step provides credibility and inertia toward implementing a comprehensive alarm management system that addresses the entire lifecycle as resources and time permit.

Because up to 80% of all alarm activations originate from a dozen or fewer sources (reference: Tips for Starting an Alarm Management Program), commonly called nuisance or bad actor alarms, addressing these alarms can significantly improve system performance.

Process alarm systems are intended to provide operational awareness and assist operators in the diagnosis and remedy of abnormal conditions, reducing incidents and accidents. Poorly implemented alarm systems can, however, have the opposite effect by overloading operators with too much information, causing confusion and masking core problems in need of attention.

Alarm overload is a well-documented issue that helped drive the emergence of industry standards and guidelines such as:

- ASM Alarm Management (2003)
- EEMUA 191 in Europe (2007)
- ANSI/ISA 18.2 Standard: Management of Alarm Systems for the Process Industries in the United States (2009)

Not surprisingly, given the long service life of a typical distributed control system, there are still a significant number of poorly implemented and overloaded alarm systems in operation.

Optimally, solving alarm management problems would begin with the formation of a committee that would adhere to the ANSI/ISA 18.2 standard to design and implement a robust alarm management system. But this isn't always realistic. Budgets, resources and scheduling are often earmarked for other priorities in spite of the urgency to correct this problem. There is, however, a cost-effective alternative to reduce alarm overload, improve process system performance, and maximize return on investment: The Monitoring & Assessment entry point of ANSI/ISA 18.2.

Problem Definition – A Brief History

There was a time when alarm management was simple. A process control system usually had only a few dozen alarms – maximum – and adding alarms was difficult, expensive and time consuming. Less critical information was conveyed via displays and log files. With fewer alarms to monitor on panel-mounted instruments, operators were able to act upon each alarm immediately.

Today, distributed control systems (DCS) provide simple and inexpensive mechanisms to add alarms. Vendors can quickly add thousands of alarms at default settings for instruments that are linked to a DCS, causing many installations to become "overloaded." Poor design and configuration practices, and technical staff who improperly identify and configure alarms, are the leading causes of bad actor/ nuisance alarms.

The distributed control systems of today have made it too easy to add alarms without realistic and manageable configurations.

During a DCS implementation, control engineers often set-up alarms, in bulk, on every loop. They can select default settings (e.g., high-high at 95% of span; high at 90% of span; low at 10%; low-low at 5%), sometimes all at high priority, with the intention of returning and correcting these settings during startup or during the first few months of production. Unfortunately, this follow-up action rarely occurs and alarm systems become ineffective and unmanageable.

Operators are bombarded with hundreds of alarms per hour, many of them causing an audible annunciation. They become conditioned to ignore most alarms, paying attention only long enough to silence the horn as they attempt to focus their attention on current process conditions.

The distributed control systems of today have made it too easy to add alarms without realistic and manageable configurations.

Overview of ANSI/ISA 18.2 Lifecycle

The ANSI/ISA 18.2 standard was developed to help the process industries design, implement, operate, and maintain effective alarm management systems.

Figure 2 illustrates the 18.2 lifecycle. It provides workflow processes and common alarm management terminology. Like any other well-defined engineering process, the alarm management lifecycle requires a:

- Written philosophy that states alarm management goals and objectives
- Documented engineering process to determine alarms
- Continuous improvement environment by maintaining, auditing, monitoring, and assessing the alarm system

In all process industries, safety is paramount. Because a faulty alarm system can contribute to process accidents, using the 18.2 standard helps improve safety and incident prevention, reduce unplanned downtime, and improve regulatory and best practices compliance. Adhering to the standard helps achieve the following alarm management goals:

- All alarms are configured to require an operator response or there is a consequence
- A thorough process is developed to help ensure alarms are defined and prioritized
- Alarms must be presented at a rate to which operators can respond
- It must be clear when the alarm system is not performing as intended

The 18.2 standard was developed to help engineering and technical staff identify ways to improve alarm management systems. It excludes information about how to implement and/or improve these systems in the most effective and economic manner.

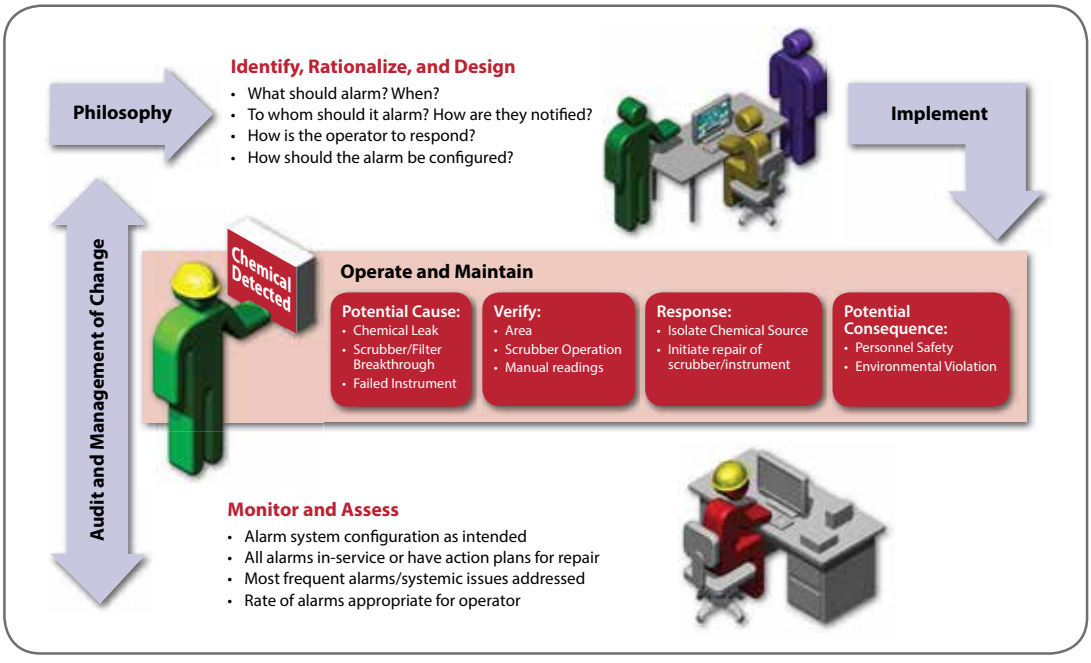


Figure 2

Monitoring & Assessment: The "Bad Actor" Solution

When dealing with bad actors and resolving the problems they present, it is best to utilize process control and industry experts.

The primary steps that are taken during Monitoring & Assessment to eliminate bad actor/nuisance alarms include:

1. Identifying bad actors with reporting software
2. Comparing them with recommended KPIs (Key Performance Indicators) for performance targets
3. Tuning and correcting bad actor alarms

The main reason alarm systems are ineffective is because distributed control systems are plagued with bad actor/nuisance alarms. These alarms often originate from fewer than a dozen sources, are unreliable, and send inaccurate information to operators. They may include chattering, fleeting, duplicate, or stale alarms, which are defined as follows:

Chattering Alarms – Chattering alarms transition into and out of alarm status in a short amount of time, often multiple times per minute.

Fleeting Alarms – Fleeting alarms transition in and out of alarm status, but they do not necessarily repeat.

Duplicate Alarms – There are two types of duplicate alarms. Dynamic Duplicate Alarms occur when a process event triggers multiple alarm annunciations in different ways. Configured Duplicate Alarms occur because incorrect DCS setpoint interconnections cause duplicate alarm configurations.

Stale Alarms – These alarms remain "in alarm" for extended periods, with case examples of 24 hours to multiple years.

All of these alarms are common and very distracting to operators. During the Monitoring & Assessment entry point, alarm system performance is measured against KPIs to identify problem (bad actor) alarms.

Identifying Bad Actors

There are several ways to analyze and identify the bad actor types. As a first step, standard alarm reports that are provided by most distributed control systems provide valuable information. For example, FactoryTalk® VantagePoint® reporting software from Rockwell Automation (Figure 3) provides standard out-of-the-box, web-based Alarms and Events reports, including:

Alarm Distribution – Identifies the alarm load impact of the10 most frequent and longest alarms.

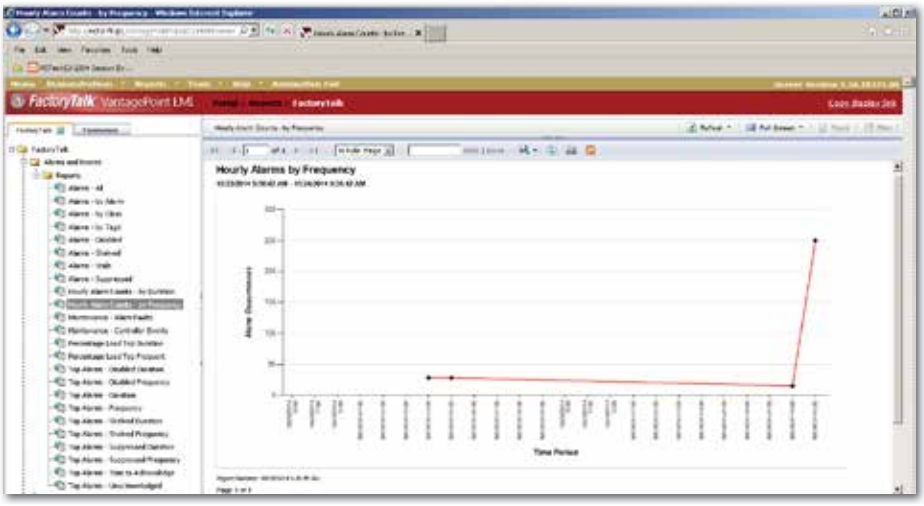
Alarm Duration – Identifies the top 10 longest duration alarms in a specific time period.

Alarm Frequency – Shows the top 10 most frequent alarms in a specific period.

Hourly Alarms – Shows a count of alarms that were active over a one-hour sample during a time period.

Standing Alarms – Shows the top 10 alarms that are currently active; determined by the length of time the alarm has been active.

Comparing the data from these reports to the recommended 18.2 alarm system target rates for Key Performance Indicators (listed below) will provide a measure of how well alarm system performance aligns with acceptable performance limits.



Very Likely to be Acceptable

- 150 Alarms per day
- 6 Alarms per hour (average)
- 1 Alarm per 10 minutes (average)

Maximum Manageable

- 300 Alarms per day
- 12 Alarms per hour (average)
- 2 Alarms per 10 minutes (average)

Figure 3

Comparing Report Data with Key Alarm KPIs

Based on the 18.2 Standard and EEMUA Guidelines, the three key alarm KPIs with acceptable targets (See Figure 4) are:

- Average Alarm Rate: < 1 Alarm / 10 Minutes
- Maximum Alarm Rate: < 10 Alarms / 10 Minutes
- Percentage of Time Alarm Rate is Outside the Limit: < 1%

Alarm Performance Metrics

Based upon at least 30 days of data

Metric	Target Value	
Annunciated Alarms per Time:	**Very Likely Acceptable**	**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%
Percent contribution top 10 most frequent alarms to overall alarm load	<1% to 5% maximum, with action plans to address deficiencies
Quantity of chattering and fleeting alarms	Zero, action plans to correct any that occur
Stale Alarms	Less than 5 present on any day, with action plans to address
Annunciated Priority Distribution	3 priorities: 80% Low, 15% Medium, 5% High or 4 priorities: 80% Low, 15% Medium, 5% High, <1% "highest" Other special-purpose priorities 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 MOC

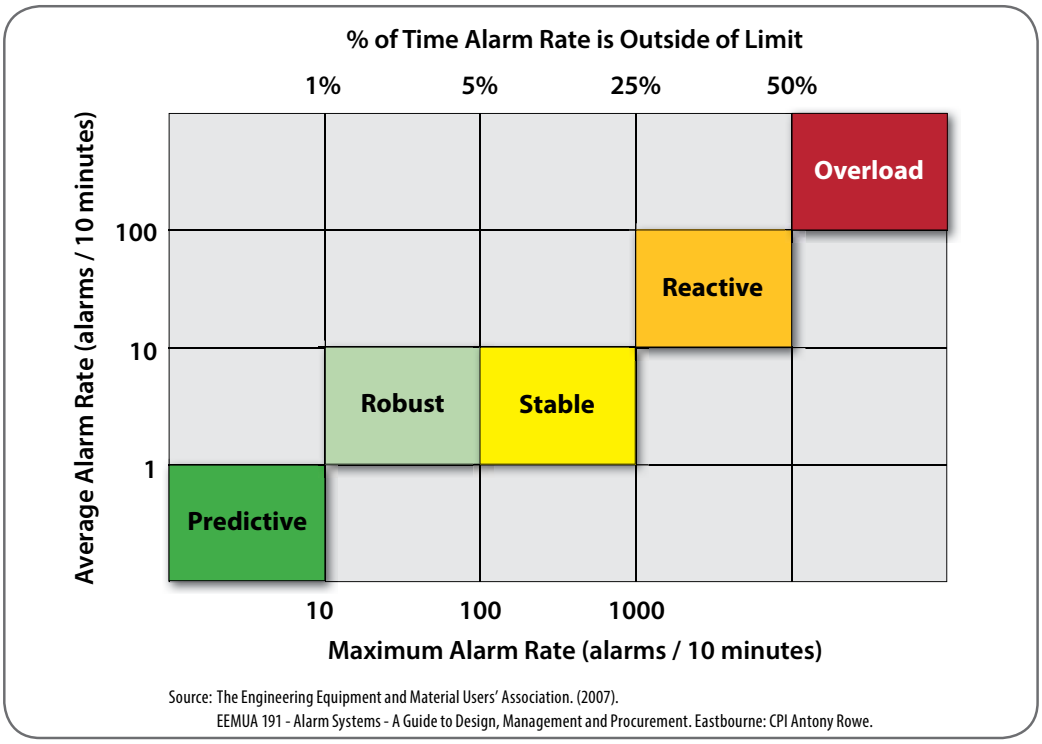
Figure 4

Other useful Alarm KPIs identified in Monitoring & Assessment, and acceptable targets for each, include:

- Top 10 most frequently occurring alarms: < 5% of Total (over 30 days)
- Number of long standing / stale alarms: < 5 with plans to address the problem
- Chattering alarms: 0
- Number of alarm peaks per time period (alarm floods): 10 alarms/10 minutes <1%
- Priority distribution of alarms: 80% low priority; 15% medium priority; 5% High priority
- Number of alarms per operating position: 6–12 alarms/hour

Note: Alarm rates that are cited are per operator/per operating location.

Managing the bad actor alarms during Monitoring & Assessment (See Figure 5) can quickly transform an overloaded DCS to the Reactive status. Employing recommendations of the 18.2 Alarm Rationalization Audit (addressed in the third white paper of this series) can move the system into either the Stable or Robust categories. Predictive systems usually require adhering to the entire 18.2 standard and implementing extensive advanced alarming techniques.



Source: The Engineering Equipment and Material Users' Association. (2007). EEMUA 191 - Alarm Systems - A Guide to Design, Management and Procurement. Eastbourne: CPI Antony Rowe.

Figure 5

Achieving the Reactive status following Monitoring & Assessment helps ensure safe operation of the DCS and eliminates many of the bad actor alarms that undercut requirements for safe operation, such as:

- Identifying and defining hazards
- Ensuring equipment is properly installed and operated
- Responding to alarms with correct procedures
- Implementing emergency plans
- Monitoring alarm system performance

Tune and Correct Bad Actor Alarms

The first step to tuning the alarm system is to remove the "information only" alarms. These messages should be conveyed by displays and log files. Next, evaluate and tune controllers and evaluate and adjust alarm limits.

The following methods of alarm tuning can correct these bad actors:

- Alarm Limit Configuration
- Alarm Deadband Configuration
- Alarm Delay Time Configuration
- Alarm Latch Configuration
- Process Filter Configuration

Alarm Limit Configuration – Manufacturing processes are dynamic. Variables such as operation setpoints, equipment installation, and equipment performance change over time. Alarm limits need to be adjusted to account for these and other changes, including a maintenance change out, a new product formulation, and/or a new operating range for an aging piece of equipment.

Alarm Deadband Configuration – Alarms on analog value need to have a deadband specified – similar to setpoints and process control. If an alarm deadband is too small, any slight variation or line noise can trigger multiple alarms. Review instrument documentation and correctly configure the alarm deadband, ensuring that it is larger than any expected signal noise. For example, deadbands on flow and level signals should be about 5%, pressure signals about 2% and temperature at 1%.

Alarm Delay Time Configuration – Most distributed control systems have two types of alarm delay: ON-Delay and OFF-Delay. They are ideal for handling chattering and fleeting alarms, but each presents unique implications. A software analysis of chattering and fleeting alarm durations and intervals will help determine which method to use. ON-Delay can keep a bad actor alarm hidden from operators if the alarm fails to remain in effect longer than the delay time specified. OFF-Delay annunciates an alarm immediately. Even if corrective action is taken to eliminate the alarm, the system will not inform the operator of a return to normal state until the delay time has expired.

Alarm Latch Configuration – Discrete alarms can be configured to latch. A latched alarm will remain in alarm, even if its condition returns to normal, until an operator resets the alarm. An operator can reset a latched alarm only when the alarm condition returns to normal. This technique is effective for eliminating chattering alarms.

Process Filter Configuration – Filter algorithms are used on process control systems to reduce noise that is generated by process variable signals. This filtering often has the same effect on alarm activation as incorrect deadband configuration. If the filter time is too long, it's possible that process problems will be hidden from operators. Suggested filter time lengths are 2 seconds for flow and level signals, 1 second for pressure signals, and zero for temperature signals.

Tuning bad actor alarms is a highly effective, immediate solution for reducing alarm system overload. A limited number of alarms result in a low-cost and highly visible alarm system improvement. However, Monitoring & Assessment does not evaluate process conditions and identify root causes of DCS installation and/or hardware issues. Performance Benchmarking and developing an alarms management Philosophy document (as addressed in the second white paper of this series) followed by the Alarm Rationalization that is described in the third white paper addresses these problems.

Leverage the 18.2 Alarm State Model

If you have selected a DCS that fully implements the ISA 18.2 alarm state model, such as the PlantPAx system from Rockwell Automation, you have more options to help eliminate bad actor alarms.

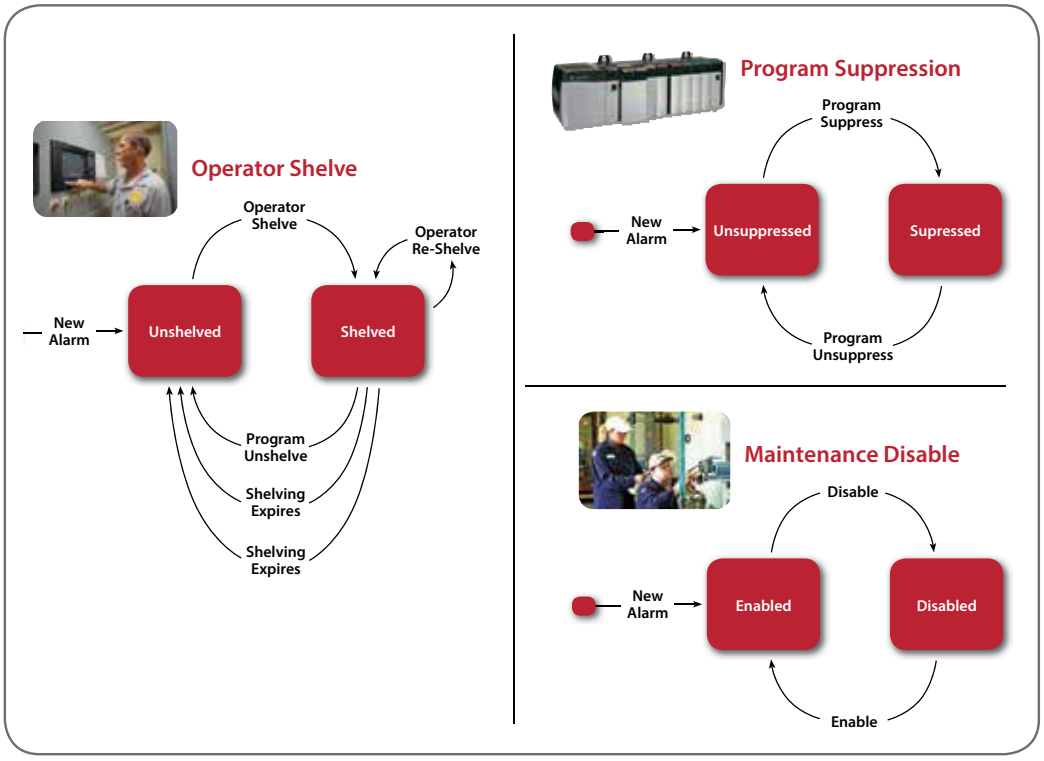


Figure 6:
Suppression type determined by process role

Shelved State

The PlantPAx system provides Shelving, a manual mechanism for an operator to suppress a potentially distracting nuisance alarm.

Shelving helps prevent alarms from being suppressed for extended periods. The maximum time that an alarm may remain in the shelved state (without being actively reshelved) is typically defined via a system default. At the time of shelving, the operator can accept the default maximum or set a lesser value. There are three ways to unshelve an alarm:

1. Operator initiated unshelve command
2. Program initiated unshelve command based on an event (i.e., shift change)
3. Expiration of the shelving timer

A shelved alarm continues to be evaluated by the system and transitions in/out of alarm. While these transitions are not displayed on the operator HMI, they are captured and logged to the alarm history.

Suppressed State

The suppressed state is used by process logic to suppress an alarm that is based on either operating conditions or plant state. The suppressed state allows a process control system to suppress/unsuppress alarms that are based on relevance. For example, alarms for a piece of equipment or plant area that is shut down can be "suppressed by design" and prevented from flooding an operator's alarm display with unnecessary information. While the alarm notification is not displayed on the operator HMI, it continues to be evaluated and logged.

Disabled (Out-Of Service) State

Maintenance staff use the disabled state when there is a need to suppress an alarm and take it out of service. This mechanism is typically used for equipment and sensors that are either in need of maintenance or removed from the control system. In the disabled state, the alarm is no longer evaluated, logged, or displayed on the operator HMI.

Storage Tank Example

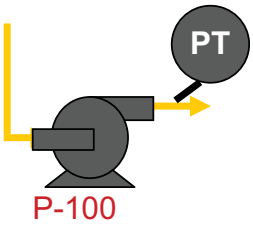
The Rockwell Automation Library of Process Objects provides effective mechanisms for dealing with bad actor alarms. By implementing the full ISA 18.2 state model, operators are provided with an alarm shelving mechanism. In addition, each Process Library object capable of alarming is programmed with common P_ALARM and P_GATE instructions that have a rich delay and suppression capability.

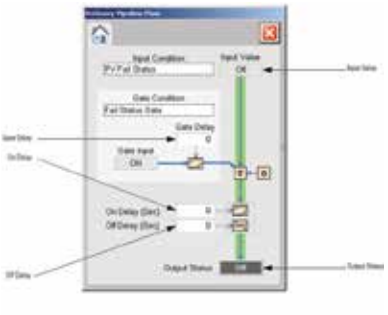
Consider a pump that is designed to alarm on low discharge pressure (an indication of a process supply problem). This alarm would be triggered whenever the pump is shut down (nuisance) and if the pump were used only periodically the alarm would not clear (stale).

An Alarm Frequency report of a Stale Alarm report would indicate that there is a bad actor alarm.

Using state-based alarming, the operator could suppress the alarm for the time period that the pump is to remain off (Operator Shelve).

Alternatively, PUMP_RUN could be used as a Gate input to prevent low-pressure status detection when the pump is shut down (Suppression by Design).





In a PlantPAx system, there is no reason to live with a poorly performing alarm system. Simple steps can be taken – all done entirely from the HMI environment without opening the controller programming – to remove bad actors by:

- Quantifying the nuisance alarms(s) using standard reporting
- Determining the condition causing the anomaly
- Applying alarm tuning using standard Rockwell Automation Library of Process Objects features from the prebuilt faceplates

Benefits of 18.2 Monitoring & Assessment

Three of the primary benefits of the Monitoring & Assessment entry point are improved productivity, increased plant safety, and improved regulatory compliance. All three benefits help improve a manufacturing facility's bottom line with a cost-effective method for helping to eliminate up to 80% of a process system's bad actor alarms.

Improved Productivity – Poor alarm system performance negatively affects operators and operations. It's one of the leading causes of unplanned downtime. Operators waste time dealing with the confusion caused by bad actor alarms by adjusting process rates that are based on bad information or by allowing processes to continue without meeting product specifications. Effective alarm management helps eliminate waste, improve processing quality, and increase productivity.

Increased Plant Safety – Alarm flooding impairs plant safety because of possible confusion when dealing with multiple bad actor alarms in short periods of time. Operators are uncertain about which alarms require priority response. Proper alarms that are meant to prevent plant incidents become ineffective in a flood of bad actor alarms. The 18.2 standard helps provide a blueprint for effective alarm management and increased plant safety.

Improved Regulatory and Best Practices Compliance – Building upon the Monitoring and Assessment phase of ANSI/ISA 18.2 is an excellent first step toward implementing a comprehensive alarm management program that meets the 18.2 standard.

Proper alarm management is an ongoing commitment. The Monitoring & Assessment entry point delivers immediate early success, but shouldn't be the sole step for improving alarm management. When more resources are available, a comprehensive alarm management system that addresses all stages included in the 18.2 lifecycle should be implemented.

The next two white papers in this series address those stages, including Benchmarking, Alarm Management Philosophy, Alarm Rationalization, Implementation, and ongoing system Audits to ensure alarm system integrity.

References

Holifield, Bill and Habibi, Eddie: The Alarm Management Handbook, Second Edition: A Comprehensive Guide; August 31, 2010

Van Camp, Kim (Emerson Process Management) and Stauffer, Todd (PE, Exida): Tips for Starting an Alarm Management Program; published in Applied Automation; April 2013

Abnormal Situation Management – ASM Consortium: Effective Alarm Management Practices 2009

Grosdidier, Pierre (Ph.D., P.E.); Conner, Patrick (P.E.); Hollifield, Bill; Kulkarni, Sarmir: A Path Forward for DCS Alarm Management; published by Plant Automation Services, Inc.

Exida – Stauffer, Todd (Director – Alarm Management Services, exida): You Asked: Alarm Management - Setting a new Standard for Performance, Safety, and Reliability with ISA-18.2; published in Canadian Process Equipment & Control News; December 2009

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication PROCES-WP013B-EN-P – June 2017
Supersedes Publication PROCES-WP013A-EN-P – March 2015