White Paper

Honeywell

Honeywell Process Solutions

Alarm Management Primer

Bradley Cook
Honeywell Advanced Solutions
Bradley.cook2@honeywell.com

Table of Contents

Introduction

The field of Alarm Management & Alarm Safety Standards became formalized in 1955 with the Instrument Society of America survey Instrument Alarms & Interlocks. The Instrument Society evolved into today's modern International Society of Automation (ISA), which works globally to harmonize automation standards, certify professionals, and provide educational resources to automation professionals.

In 2009, both ISA and ANSI[1] jointly published a new standard for the management of alarms in process industries, **ANSI/ISA-18.2-2009**. This new standard represents the next stage in an ongoing process of increasing safety, reliability, and visibility on the plant floor. It complements the already well-established EEMUA[2]-191 guidelines for Alarm Systems. ANSI/ISA 18.2-2009 establishes clear standards for the overall lifecycle of alarm management, accountability, and reporting.

ANSI/ISA 18.2-2009 signals a fundamental change in the ways businesses operate their plants. This new standard impacts regulatory and reporting requirements, with particular emphasis on the following industries: Oil & Gas, Power, Nuclear, Commodity Chemicals, Petrochemical & Refining, Mining & Minerals, Pharmaceuticals, Food & Beverage, Pulp & Paper, and Discrete Manufacturing.

Who Should Read This Document?

This Document is intended to provide plant engineers, operators, and managers with some of the basic considerations associated with starting an Alarm Management programme. Ideally, it will help them scope out some of the functional requirements and get a sense of how well they are performing.

It is not intended to be comprehensive guide to the field, or even a step-by-step set of instructions to achieving compliance. A good alarm management programme will always require good engineering practices. A good starting point would be to purchase and read the published standard itself.

This is not a review of the ISA standard, however it will be referenced as appropriate.

What Is An Alarm?

> A process alarm is defined as *an audible or visible means of indicating to the operator, an equipment or process malfunction or abnormal condition requiring a response. (Source ANSI/ISA-18.2-2009)*

Too often we see situations where the alarm system is used as a messaging system, to provide the operator with information that is redundant, does not require a response (other than an acknowledgement), or may represent a perfectly normal operating condition.

[1] American National Standards Institute
[2] Engineering Equipment & Material Users' Association

What Is Alarm Management?

> *The process by which alarms are engineered, monitored, and managed to ensure safe, reliable operations.*

Before the wide availability of computers in alarm systems, control panels had limited space and each alarm required significant engineering (and associated cost) to implement. Computer controlled alarm systems reduced the cost of implementation to near-zero, leading to ongoing and significant profligation of alarms in the system. Compounding the issue, many alarms serve no purpose. As the numbers of alarms increase, and their quality decreases, operators lose the ability to respond effectively, leading to potential safety, environmental, or business losses.

By implementing a consistent, auditable, and cyclical process of managing the underlying practices of alarm performance, review, and maintenance; plant operations can ensure good engineering practices within the alarm system.

The Real Cost of Doing Nothing

The new standard establishes a level playing field in the practice of alarm management, across industries and regardless of size. Yet it is flexible enough to allow each business to establish its own performance criteria and set of metrics, subject to their own business requirements.

The sad truth is that the drive to standardization of alarm management practices was as a result of several high-profile incidents that lead to loss of life, environmental releases, equipment damage, and loss of production. Each instance of a bad alarm distracting an operator can be considered a form of safety violation, exposing the business to risk of health & safety incidents, environmental incidents, fines, and even criminal prosecutions.

Beyond this, a poorly performing alarm system also leads to ongoing and incremental operating costs that are hidden from ordinary review. For example, a plant may be paying too much in insurance if their alarm safety system is out-performing industry averages and they cannot document it.

Other examples:

1. Operators may be diverted from their primary role to spend time investigating and responding to nuisance alarms.
2. As a result, operators don’t have enough time to optimize unit operation (implied higher production costs). In fact, it is not unusual to find situations where operators deliberately slow operations so that they can keep up!
3. Asset performance: it is the operators who are in ready, day-to-day contact with critical assets. Without adequate time and tools to monitor ongoing trends in asset performance, operators are left to wait until problems arise before calling maintenance (which often as not leads to inconclusive results).

The Alarming Truth about Alarms

Plant management may be surprised to learn that their alarm system is not only operating sub-par, but actually represents significantly more business risk than they imagined. This does not necessarily mean that their plant is in danger of an impending incident. Business risk is a real cost that affects all aspects of the operation; having the alarm principles, business practices, and performance monitoring tools in place to effectively measure ongoing operational risk with respect to the alarm system enables

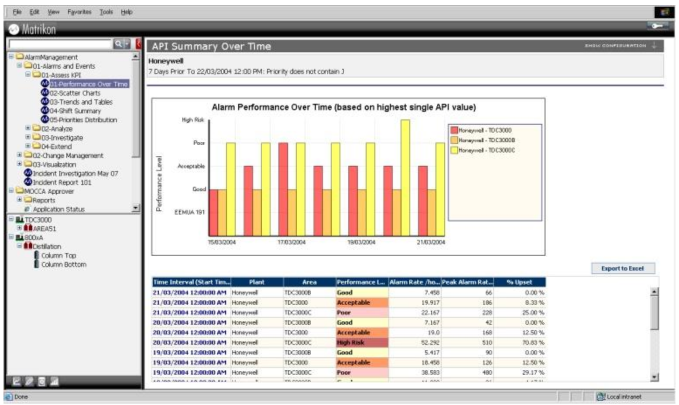


Figure 1 - Alarm Performance

management to implement better strategies around real issues that affect the plant every day.

Where to Begin?

"A journey of a thousand miles begins with the first step." In this case, the first step is a broad scoping question. It is a matter of data collection and an assessment of current performance against industry practices. Oftentimes, this can be done at little or nor cost, as much of the relevant data may be archived in the plant historian.

Where there are gaps in data or inadequate histories, setting up a temporary archive to collect and store relevant alarm performance information (e.g. 1-3 months) will act as a suitable alternative. Commercial off the shelf (COTS) tools will help in the generation of alarm system performance reports:Peak Alarm Analysis

- Average Alarm Rates
- Percentage Upset
- Priority Distribution
- Top 20 Alarms
- Standing Alarms
- Chattering Alarms
- Symptomatic Analysis

- Operator Intervention Analysis
- Further Recommendations

Defining Expectations

When are alarms needed in my plant? When are alarms not needed? What actions are required following an alarm? What about maintenance? Or Training?

The ISA standard requires that all plants document precisely how they will employ to manage their alarm systems. This engineering document, called the **Alarm Philosophy** becomes the yardstick against which all future performance is measured. At the very least, an Alarm Philosophy Document should cover the following details:

- Purpose
- Definitions
- Roles & Responsibilities
- Design Principles
- Rationalization
- Alarm Class Definition
- HMI Design
- Prioritization
- Performance Monitoring
- Maintenance
- Testing
- Implementation Guidance
- Management of Change
- Training
- Alarm Histories

The Rational Alarm

The process of Alarm Rationalization is the systematic review and documentation of alarm settings and engineered requirements. Each alarm-able tag must be systematically reviewed with the objective of optimizing alarm quantity and quality. Each alarm should have documented causes, consequences, and corrective actions. A rationalization exercise can be resource-intensive, with cumbersome logistics (e.g. need to book availability of different operators from different sections). If any part of the exercise faces delays, it has a cascade-effect on all downstream activities. The general methodology (per tag) is:

1. Should there be an alarm?
2. What should the limit be?
3. What is its priority?
4. Should there be different settings for different plant modes?

Practically, the process of rationalizing alarms means populating a large database with all the requisite information for each alarm. This Master Alarm Database stores all the engineered values for all alarms. Such a database can easily be built using common tools like a spreadsheet; however such an implementation will limit it to one-time-use. A better way would be to use Matrikon MOC which can fulfill multiple roles, including acting as Master Alarm Database, provide ongoing discrepancy reporting (e.g. alarms set outside of engineered limits), provide one-click online documentation for all alarms, and provide an audit trail of changes to the alarm system in support of plant-wide management of change procedures.

Quantity vs. Quality

Many plants periodically attempt to clean-up chattering and/or standing alarms, in hopes of improving performance. However they often overlook alarm quality. Quality represents the grades of alarms (HI, MED, LO), the number of variations, and identifying if each and every occurrence of a HI priority alarm is truly of greater importance than MED and LO priority alarms.

Setting Alarm Priorities

Alarm priorities are driven by severity and time to respond. It is essential to remember that each alarm must have a rational consequence associated with it (consequence of doing nothing, e.g. plant trip). Severity is typically indexed by impact category and level. The Impact Category is based upon business priorities (e.g. personnel, environmental, equipment, production cost), whereas level can be a simple grading (e.g. minor, moderate, severe). Levels should be consistent across categories and consistent with corporate direction.

Likewise, the impact of time to respond on alarm priorities means that potentially severe events do not ring through as impending emergencies unless they really are impending.

The ISA standard recommends limiting Priorities to only 3, or 4 overall to reduce the potential for confusion in critical situations.

Management of Change

Changes to alarm system settings are often *ad hoc*, poorly documented, and performed without formal authorization. While such practices may seem expedient at the time, they too-often lead to alarm setpoint changes outside of engineered values, permanently (lost) inhibited alarms, or unnecessary alarms. ANSI/ISA-18.02-2009 places heavy emphasis on plants employing (and enforcing) Management of Change (MOC) procedures for alarm systems.

- Adding or removing alarms must be authorized via the MOC
- Alarm setpoint/design changes must be assessed through MOC, including:
    - Technical justification
    - Impact on HSE

    - Conformance with APD
    - Any changes of operating procedures
    - Valid applicable period
    - Authorization requirements
    - Safety assessment
    - Personnel requirements (e.g. training)
- Mandatory documentation for changes via MOC must include:
    - Reason for the change
    - Date
    - Name(s) of implementors
    - Name of authority
    - Nature of change
    - Training requirements
    - Testing requirements

Picking the Team

So who does it? Who "owns" alarm management?

To be effective, it really needs to be owned by operations, and driven by the operators. They will be using it, they will be receiving the immediate benefits, and they will be on the front lines when push comes to shove.

To perform the actual rationalization, it is not advisable to hire a co-op student to be responsible for this project; this is a recipe for failure. Ideally it will be include an experienced operator. This is the person with the war stories and their finger on the pulse of the system.

A process engineer is also a critical team member. The operator may be unaware of each and every alarm. The process engineer brings Hazop and Process-Op knowledge to the table and will help ensure that the removal of any alarms is in line with best practices.

Controls engineers from various sites/areas will be required, but not all the time. It is important to understand on a site-by-site basis the performance abilities of each control system and its limitations. For example, it may seem obvious to come up with a dynamic alarm suggestion, but actual implementation may not be practicable, due to time, cost, or other constraints.

A facilitator/ coach will help the team stay focussed and ensures that progress is accountable. A strong facilitator will be able to advise the team on industry best-practices and make recommendations. This does not have to be an external person, but <u>must</u> be somebody experienced in the process of alarm rationalization.

A project manager may be useful, particularly at the beginning of the project.

In a plant with multiple areas/sites, all team members will not be required all the time.

Performance Targets

There are several key performance indicators that need to be tracked to ensure your a rationalized alarm system is maintains international standards. As with any engineered system, over time its performance will degrade and the degradation will compound. By tracking a few key metrics, plants will have a clear reference of alarm system performance compared with international standards. Any gross deviations should be followed up with a mandatory review and action plan.

Here is a list of several performance targets specified in ANSI/ISA-18.2-2009.

Alarms / day	150
Alarms / 10 minute period (target)	1
Alarms / 10 minute period (max manageable)	2
Percentage of hours in burst (>30 alarms/hr)	<1%
Max alarms / 10 min	10
Percent of time in flood	<1%
Max allowable chattering/fleeting alarms	0
Percent contribution to top-10 alarms	1%
Stale alarms	5/day
Alarms suppressed outside of MOC	0
Alarm attributes changed outside of MOC	0

Table 1 - Alarm System Performance Targets per Operator

There are a couple of unstated implications to these performance targets.

1. Plants are free to deviate from these recommended targets and substitute their own targets, if the define those substituted targets in their Alarm Philosophy and document the rationale behind it (e.g. In-house human-factors engineering study, abnormal situation simulations, industry-specific alternate standards). Plants that fail to adequately justify a deviation could be subject to sanctions from a regulatory authority during an enforcement activity, such as an OSHA incident investigation.

2. Having performance targets is one thing, but being able to monitor and document that the plant is meeting the targets on a regular basis requires specialized tools. More importantly, having the procedures and workflows in place to be able to act on discrepancies as they arise closes the loop on reporting and will help ensure long-term sustainability.

Operator Tools

As previously mentioned, alarm management is “owned” by the operators. They are the primary clients and their needs drive the requirements. Effective interaction with alarm management tools and the ability to leverage the technology for operational improvement are essential in any facility. This is beyond the standard HMI alarm interface available on most control panels.
The operator needs to:

- Understand & support the goals and objectives of the alarm management programme
- Input, update, and have timely access of alarm assistance information (IE. The operator needs immediate and timely access to causes, consequences, corrective actions and any other relevant data for each an every alarm, no matter how infrequent)
- Understand and log the impact of poorly performing alarms on the facility
- Effectively process and manage the real-time information of an alarm system
- Understand and support the Management of Change processes for the effective maintenance of the alarm system
- Fully leverage the Alarm & Events historical database for improved operational performance
    - Shift Change Reports
    - Reports for Outside Operators
    - Incident Capture
    - Training Review

On-the-fly searching, filtering, sorting, and querying of real-time alarms gives operators the power to zero-in on potential trouble spots before they become critical. Figure 3 shows an example Sequence of Events (SOE) screen in real-time; the operator can instantly click on any alarm to bring up its full history, with searches of past occurrences to look for similarities or patterns on previous occasions.

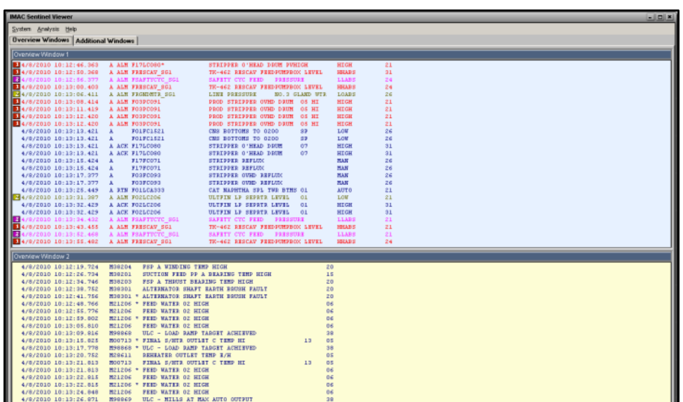


Figure 3 - Real-Time Multi-Source Sequence of Events Report

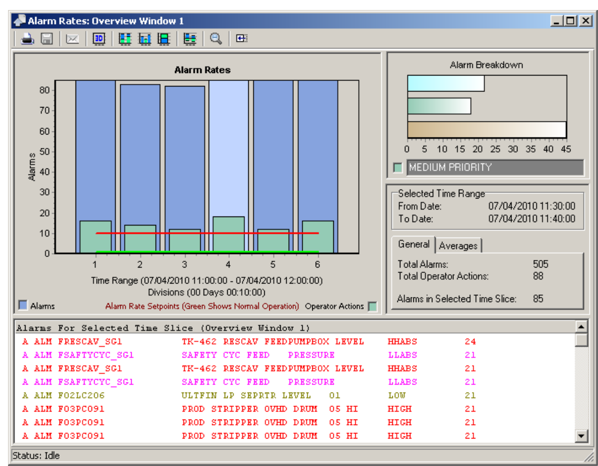


Figure 2 - Sequence of Events Alarm Rate Report

Supervisory Tools

The role of the Operating Supervisor is to review dynamic alarm system performance on a regular basis, typically daily or weekly. The supervisor's objective is to ensure that performance targets are met and that any deviation from desired benchmarks is related to specific unit-level operating problems. Supervisors also like to ensure that these benchmark performance metrics are visible to the operating and maintenance teams, such that they can more-easily provide corrective action and re-establish compliance. Useful supervisory reports include:

- Average Alarm Rate
- Peak Alarm Rate
- Percent Upset
- Standing Alarms
- Operator Action Rate
- Operator Actions : Alarms Ratio
- Top 20 Alarms
- Top 20 Actions
- Priority Distribution

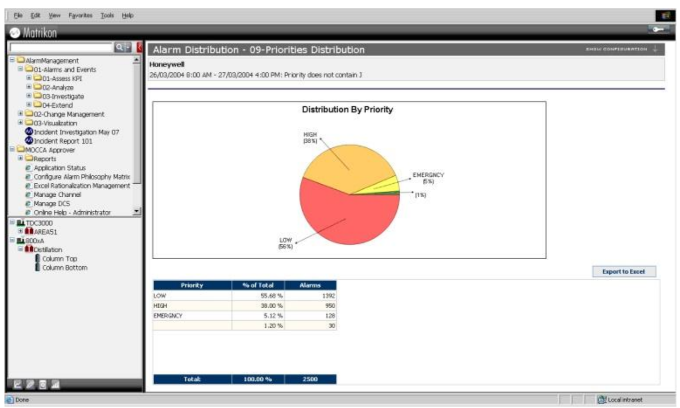
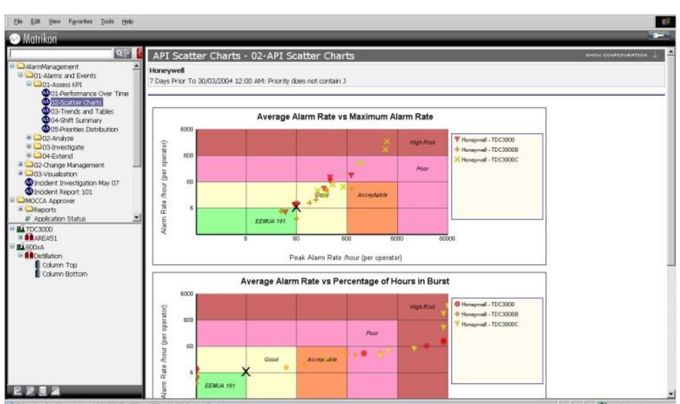


Figure 4 - Alarm Priority Distribution Report

Plant Management Tools

High-level alarm performance reports consolidate facility/ unit level alarms into an indication of overall plant operating stability and safety. For example, a high level scatter-chart indicating plant stability in context of critical metrics.



A plant operating in an **overloaded** state is experiencing peak alarm rates and average alarm rates beyond which current operator(s) cannot effectively process alarm information in a safe and reliable manner. It suggests that alarm information is of questionable value and that the plant is at risk of serious incident.

A plant is considered **reactive** when both the peak alarm rate and average alarm rates are still too high, but the operator(s) can reliably process a limited amount of alarm information. Alarms are somewhat manageable, but the plant is still exposed to risk of a serious incident.

A plant that is **stable** with respect to its alarm system has its nuisance and chattering alarms under

Figure 5 - Overall Plant Performance Scatter Chart

control and alarm rates are acceptable during normal operations, however the system is less useful during plant upsets, when the alarm safety system is needed most. It is somewhat susceptible to missed alarms and/or incidents.

Plants operating in a **robust** state experience alarm rates such that operator(s) can effectively process all incoming information; they have ample time to relate alarm system information to required operating actions. Both the average and peak rates are under control.

Predictive control is the ideal target of ANSI/ISA-18.2-2009. Dynamic alarm allows for different alarm limits based upon plant state and operators have ample time to optimize overall performance in order to achieve maximum benefit.

Engineering Tools

Properly historized and cross-indexed A&E data is extremely useful for engineering support:

- Integrated A&E data with process data directly in the historian tool set
- Integrated reliability analysis with supporting data from the A&E database
- Analysis of the impact of process upsets or poor unit performance on overall profitability

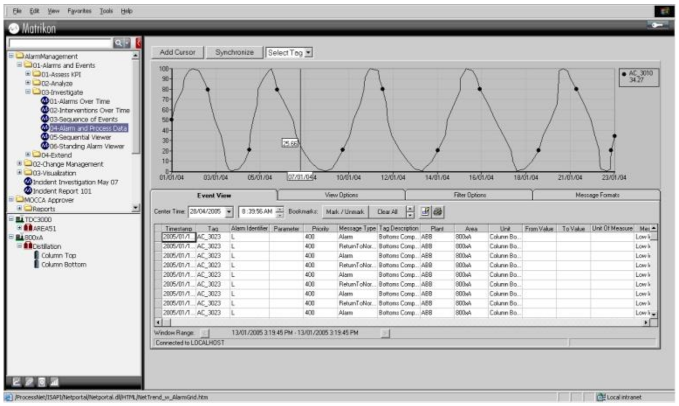


Figure 6 - Correlated Process & Alarm Data

Additional Tools

Health, Safety, and Environmental personnel benefit from simplified access to critical alarms and automated reporting of key incidence. This accelerates compliance reporting, helps quickly identify and troubleshoot environmental/safety alarms, and provides a secure database for post-audit analysis.

Human Resources personnel also receive better metrics for optimizing staffing requirements. The A&E database contains the information required to best assess and optimize panel operator staffing. This will help assess the impact of operator attrition, control room consolidation, new unit integration, and tracking of training requirements.

Alarm Manager – Powered by Matrikon

Matrikon Alarm Manager is an integrated alarm management software solution. It is the most widely installed process control alarm management software, providing comprehensive alarm management capabilities; including:

- Alarm and Event archiving
- Alarm and events analysis
- Alarm Enforcement
- Auditing and Traceability

Matrikon Alarm Manager provides for open-connectivity and vendor independence. This allows for apples-to-apples comparisons of alarm performance across various units of the plant, which is especially useful when there is a mixed set of control systems from multiple vendors. Alarm Manager is built using open technology standards; including, service oriented architectures, MSSQL, and other emerging technologies thus providing the ability to connect to any of your control systems.

Summary

Responsible practices in alarm management require plants to engineer and maintain alarm systems, measure their performance, conduct regular reviews, and remediate as necessary. These efforts do not need to be onerous if practiced as part of a normal routine, as may be employed with any engineered system. It is all the more important to do so with alarm systems, as their maintenance is vital to plant safety, optimal operational performance, and regulatory reporting.

In a situation where the plant alarm system has been allowed deteriorate to the point where it poses significant risk, the process of remediation may seem daunting at first. Industry best-practices defined by global standards and enforced by regulatory authorities provide a clear path and expectations for ongoing efforts. Leveraging proven tools and solutions will help plants save time, money, and reduce risks associated with poorly managed alarms.

Consulting with subject matter experts will add clarity and provide insight into best-practices per industry – for example, what works for a mining operation may not work for a gas pipeline. Matrikon technology & expertise is now part of Honeywell Advanced Solutions, making us the world's largest provider of advanced software and services to the process industries. Our solutions Powered by Matrikon offer universal connectivity, underlying system & application independence, and greater ERP integration

References

- ANSI/ISA-18.2-2009 "Management of Alarms in the Process Industries"

- EEMUA-191 "Alarm Systems - A Guide to Design, Management and Procurement"

- Abnormal Situation Management Consortium White Paper: Common Operations Failure Modes in the Process Industries, Bullemer, Laberge.

- ASM Resources: www.asmconsortium.net

- Matrikon White Paper: Alarm Management Standards – Are You Taking Them Seriously?, Baade.

More Information

For more information about Honeywell's products/ solutions, visit our website at
www.honeywellprocess.com
www.matrikon.com
or contact your Honeywell account manager.

Automation & Control Solutions
Process Solutions
Honeywell

1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Arlington Business Park
Bracknell, Berkshire, RG12 1EB

Shanghai City Centre, 100 Junyi Road
Shanghai, China 20051

www.honeywellprocess.com

WP-12-xx-ENG
Month 2012
Printed in USA

Honeywell