ALARM MANAGEMENT STANDARDS

Honeywell

TABLE OF CONTENTS

DOCUMENT TERMINOLOGY

NAME	DEFINITION
AMTF	Alarm Management Task Force
API	American Petroleum Institute
ASM	Abnormal Situation Management
CHAZOP	Control/Computer HAZOP
DCS	Distribute Control System
EEMUA	Engineering Equipment Material Users Association
FTA	Fault Tree Analysis
HAZOP	Hazard and Operability Study
HMI	Human Machine Interface
HSE	Health and Safety Executive
IEC	International Electrotechnical Commission
ISA	International Society of Automation
KPI	Key Performance Indicator
LOP	Layers of Protection
MOC	Management of Change
OH&S	Occupational Health and Safety
PFD	Probability of Failure on Demand
PHA	Process Hazard Analysis
PHMSA	Pipeline and Hazardous Materials Safety Administration
PLC	Programmable Logic Controller
SIL	Safety Integrity Level
SIS	Safety Integrated System

MANAGEMENT SUMMARY

> **More than 30 years after Honeywell formed the Alarm Management Task Force, an advisory board comprised of key customers and led by Honeywell to document the issues associated with Alarm Management, many companies still do not have a formal Alarm Management program or take the issues associated with Alarm Management seriously.**

Employers, irrespective of the size of the business or industry sector, have responsibility for the day-to-day health, safety and welfare of employees, visitors to the workplace, and the surrounding community at large. This duty of care is usually set out in the occupational health and safety (OHS) legislation of the relevant country. Duty of care usually mandates that employers of process and other automated industries provide a suitable alarm system that gives adequate warning of impending abnormal situations to operators, so they have time to take action to prevent the potential consequences from occurring. Duty of care also includes the provision of a control system that does not put the operators under undue levels of stress, which could also compromise the safety of other employees.

When companies fail to do this or fail to take seriously the recommendations of international standards organizations designed to help address these issues they create an environment that is more likely to experience unnecessary and often avoidable abnormal situations, some of which may put people, the environment, and profits at risk. Corporate executives are accountable to their stakeholders for these abnormal situations and companies as well as individuals from Supervisor to CEO level have been legally prosecuted for industrial accidents and breaches in safety and/or environmental regulations in some countries. Because of this and the potential liability associated with industrial incidents, it has also been noted that in recent years some insurance companies have threatened to increase premiums on plants that do not initiate or maintain an active alarm management program, or have offered discounts or incentives to those who do.

In 1999 EEMUA published the first edition EEMUA Publication 191 "ALARM SYSTEMS - Guide to Design, Management, and Procurement". Since that time other standards have emerged and today the three leading contenders for Alarm Management Standards are; ISA 18.2 "Management of Alarm Systems for the Process Industries" (2016), EEMUA Publication 191 Edition 3 "ALARM SYSTEMS - Guide to Design, Management, and Procurement" (2013), and IEC 62682 "Management of Alarm Systems for the Process Industries" (2014) which was adapted from ISA 18.2 (2009). ISA 18.2 and EEMUA 191 are acknowledged as the defacto standards for Alarm Management and IEC 63683 is seen as an International Standard based on ISA 18.2. Each of these publications have similar KPIs for alarm system performance, define similar work processes, and recommend the same Alarm Management Lifecycle. So, what does this mean for your industry?

This paper provides an overview of what alarm management is and why it is important. It also provides insight into these global standards, and what you can do to achieve compliance.

WHAT IS ALARM MANAGEMENT?

DEFINITION OF ALARM MANAGEMENT

The EEMUA 191 definition of Alarm Management is "The processes and practices for determining, documenting, designing, monitoring, and maintaining alarm system" to ensure safe, reliable operations. This simple definition encapsulates the primary function of an alarm management system but only scratches the surface of what is required to ensure that your alarm system meets the relevant standards which are increasingly relied on as the basis for modern alarm system configuration.

The primary function of the alarm system is to ensure that operators are notified of an abnormal situation that requires actions be taken to prevent or mitigate the potential consequences that could occur if the abnormal situation goes undetected. This makes Alarm Management an essential layer of protection.

LAYERS OF PROTECTION

The concept of Layers of Protection is to provide Independent Layers of Protection around hazardous processes to reduce the risk of undesired consequences such as fire, toxic releases etc. (Refer to Figure 1). Alarm Management is, therefore, a Layer of Protection (LOP) and often used in Safety Integrity Level (SIL) analysis. The intent of these alarms is to warn operators of an impending abnormal situation, which can often have safety related consequences. In determining the average Probability of Failure on Demand for a SIL loop that contains an alarm as a LOP, the probability of the operator failing to adequately respond to the alarm must be considered. Some plants assign an unrealistic probability of failure, especially where the alarm rates have been over the "maximum manageable" metric as identified in the EEMUA 191 and ISA 18.2 standards. This has the potential to make the SIL design for a loop inaccurate. How do these standards impact the design of an Alarm Management System?

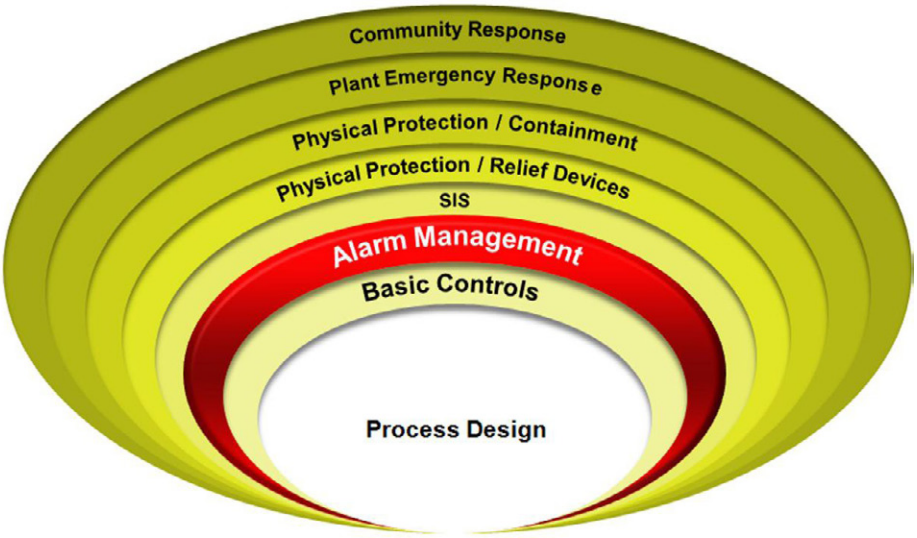


Figure 1: Layers of Protection in a Processing Plant

ALARM MANAGEMENT STANDARDS

There are several Alarm management Standards targeted to various industries. Starting with the Alarm Management Task Force (AMTF), a customer advisory board led by Honeywell in 1990, this group of industrial control system users quickly realized that alarm management issues were part of a bigger problem. This led to the formation of the Abnormal Situation Management Consortium or ASM™ (ASM is a registered trademark of Honeywell). The ASM Consortium researched numerous factors that impact how configuration of the alarm system impacts the operator's situational awareness and ability to identify and react to abnormal situations.

The ASM Consortium published numerous documents over the years on best practices in alarm management, operator effectiveness, and operator situation awareness, many of which are available for download (see www.asmconsortium.org for more information). The ASM Consortium also contributed to the creation of the first version of EEMUA 191 by providing data from member companies and editing of the standard prior to it's first publication in 1999. Since that time two standards have emerged as the primary guides for Alarm Management;

- ISA 18.2-2016 "Management of Alarm Systems for the Process Industries" (2016)
- EEMUA Publication 191 "Alarm Systems – Guide to design, management and procurement" 3rd Edition (2013)

Other notable standards include;

- IEC 62682 "Management of Alarm Systems for the Process Industries" (Published in 2014 as an internationalized adaptation of ISA 18.2)
- API 1167 – "Pipeline SCADA Alarm Management" (2010)
- PHMSA (CFR 192.631/CFR 195) – "Control Room Management for gas and hazardous liquid" (2009)

WHY IS ALARM MANAGEMENT IMPORTANT?

In a nutshell: People, Planet, Profits.

PEOPLE: Protecting the safety of employees working in and around processing plants and the community at large is the responsibility of the company and its management. This is also the primary function of any alarm system, which must be configured to identify situations that may pose a health or safety risk and to notify operations personnel in time to allow them to ensure the situation is addressed and personnel in the area are alerted to the hazard.

PLANET: Increasingly environmental releases of any kind carry with them a potential risk to the health of people both within and outside the confines of the plant as well as hefty fines from environmental regulatory bodies. Harm to the planet's environment has become nearly as important to avoid as harm to personnel in and around the plant. The installation of sensors and analyzers to monitor processes which may potentially release chemicals into the environment has dramatically increased in recent years. Alarm systems must be configured to recognize and alert operations to conditions that might lead to a potential release of a regulated substance.

PROFITS: Stakeholders in any plant have invested time, reputation, and resources to develop and/or operate a facility that delivers profits to its stakeholders. A poorly configured alarm system more frequently leads to unnecessary shutdowns, quality issues, equipment damage and production deferment all of which have an impact on profitability. In addition, the previous risks to People and Planet each have the potential to carry significant and often crippling financial impacts from fines or litigation.

No senior manager or corporate executive wants a failure in one of these areas to occur on their watch. Add to this the risks that a failure in any of these areas poses to the reputation and viability of a plant, especially in a highly competitive market, and the importance of a good Alarm Management strategy that is competently implemented and consistently maintained is increasingly obvious and necessary.

Abnormal Situations cost industry millions or even billions of dollars every year. Over the last several years there have been a number of plant incidents that have been partly attributed to poor alarm management practices which have tragically resulted in injury and death of personnel, significant environmental impact, and huge financial losses. Some examples are the Longford Gas Explosion in 1998, the Texas City Oil Refinery Explosion in 2005, and the Deepwater Horizon Oil Platform in 2010 which not only claimed 11 lives but has cost BP over $60 billion dollars in fines, settlements, and lost production and created the worst environmental disaster in U.S. history.

ISSUES THAT IMPACT ALARM MANAGEMENT

There are several issues that can impact the effectiveness of an Alarm Management system. Any one of these has the potential to severely impact the alarm system and the operator's situational awareness as a result. Alarm rates that are beyond the operator's ability to process often render the alarm system useless. High alarm rates are typically caused by one of the following issues, all of which should be identified, evaluated, and addressed.

Failure to correctly identify an Alarm

As simple as it may sound, one of the biggest problems found in most control systems is the failure to correctly identify what an Alarm is. When developing an Alarm Philosophy, one of the first things required is to provide a clear definition of what constitutes an alarm. Early control systems, that relied on panel displays, were costly to implement and difficult to change. Modern control systems rely on smart instrumentation, network connectivity and often wireless communication. This makes adding alarms much easier and far less costly. The result has been a proliferation of potential alarms many of which often fail to meet the definition of an alarm based on the industry standards.

All standards agree that an alarm must meet specific criteria before it is configured to annunciate and display to an operator. ISA 18.2 defines an alarm as an "audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a timely response". In other words, an alarm notifies the operator that something in the process has occurred which has some undesirable consequences and that requires the operator take actions to mitigate the issue in a timely manner. For example, the alarm system is not to be used to notify the operator that a pump started when it was supposed to, but rather that the pump was supposed to start but did not so the operator can take necessary actions in time to mitigate the consequences of the pump not starting.

Poor Process Control Logic and/or Configuration

Good process control assists in minimizing the probability of abnormal situations occurring due to interlock failure, incorrect logic configuration or uncontrolled PID loops. Poor process control, on the other hand, typically results in large numbers of Bad Actor alarms such as; unnecessary alarms, chattering alarms, duplicate alarms, and other nuisance alarms. This can lead to an increased number of operator actions required to control the process which can diminish an operator's situational awareness and lead to missed or overlooked alarms or standing and stale alarms. It can also result in operators shelving or inhibiting nuisance alarms for extended periods of time, often weeks or months without plans to address the underlying situation.

Equipment Malfunction or Failure

All manufactured equipment eventually fails with time. Unfortunately, some companies rely too heavily on the higher LOPs (safety systems, pressure relief valves etc.) to protect the integrity of their plants in such a case. Even safety equipment, however, has a probability to fail on demand and should only be employed as a last means of defence. Good plant maintenance practices are critical in terms of safety, plant production rates, and alarm system performance. Poorly maintained equipment or instruments can result in nuisance alarms such as fleeting, chattering, or false alarms which increase the probability of an avoidable incident occurring.

No or Poor Alarm Rationalization

Alarm Rationalization is the process of assigning an alarm's priority based on an analysis of the alarm to determine the;

- Cause of the alarm,
- Consequence if no action is taken to address the situation,
- Severity of those consequences based on the Risk Assessment Matrix,
- Maximum Time to Respond for the operator to prevent the consequences,
- Corrective Actions the operator should take to mitigate the situation.

Many companies fail to follow the ISA 18.2 or EEMUA 191 guidelines for proper Alarm Rationalization. These guidelines help ensure alarms are prioritized properly to call the operators attention to the more critical and/or time sensitive alarms in a timely manner so actions can be taken to mitigate the situation. Failure to do so can present the operator with a confusing display of alarms that hinder the operator's situation awareness and increases the likelihood that a critical alarm is missed, or incorrect actions are taken.

The result at many sites is that when the alarm system is needed most, operators ignore the alarms because they are overwhelmed with confusing information, and the alarm system becomes virtually unusable in its current state.

DEMYSTIFYING THE STANDARDS & GUIDELINES

As previously stated, ISA 18.2 was first released in 2009 and later updated in 2016 and is now widely considered the defacto standard for Alarm Management. EEMUA 191 was first released in 1999 and is in its 3rd Edition (2013). IEC62682 was released in 2014 adapted from ISA 18.2 and represents an internationalization of the Alarm Management standard. Since IEC 62682 was adapted from ISA 18.2 let's focus on ISA 18.2 and EEMUA 191.

ISA 18.2 and EEMUA 191 complement each other. ISA 18.2 clearly defines the required performance KPIs and the overall lifecycle approach to alarm management. The performance KPIs for both documents are similar, although they are more clearly defined in Table 14 of ISA 18.2, while EEMUA describes in detail the tools and techniques for various aspects of alarm management (e.g. rationalization, risk assessments, graphics design).

KEY FEATURES OF ISA 18.2 AND EEMUA 191

The main features of ISA 18.2 and EEMUA 191 are highlighted in this section.

ISA 18.2 (2016) Key Features

- Large focus on an alarm system lifecycle.
- Very clear alarm system performance KPIs.
- Written like other similar standards – e.g. IEC 62682.
- Section on conformance requirements.
- Alarm Philosophy purpose and contents.
- Alarm System requirements specification.
- Identification purpose and methods
- Alarm rationalization purpose, prioritization, classification, documentation.
- Basic alarm design, alarm types, attributes, use of deadbands and delays
- HMI design considerations, enhanced and advanced methods, requirements.
- Section on enhanced and advanced alarm methods
- Implementation planning, testing, training
- Operation, response procedures requirements and recommendations
- Maintenance, repair, replacement, periodic testing, training.
- Sections on: Monitoring and assessment, Management of change, and Auditing.
- Complementary to EEMUA 191.

EEMUA 191 (2013) Key Features

- Good detail on alarm design, including different risk assessment approaches.
- Written in an easily readable text-book format – excellent examples.
- Good discussion on Alerts vs. Alarms.
- Principles of alarm system design and structuring of alarms
- Risk assessment and using alarms for risk reduction.
- Implementation process; management organization, improvement program, assessments.
- Philosophy; purpose, contents, rules and guidance.
- HCI management techniques, alarm display options, annunciation, graphics
- Alarm configuration; processing, testing, suppression techniques.
- Alarm system improvement (rationalization) process
- Performance monitoring/improvement, Benchmark values and KPIs.
- Appendix on the costs of poor alarm performance with examples
- Appendix on alarm management in Batch Plants.
- Complementary to ISA 18.2.

KPIs for both EEMUA and ISA 18.2 are nearly identical but presented differently.

EEMUA ALARM PERFORMANCE KPIS

EEMUA suggests three main KPIs on a per operator basis for 10-minute time periods:

- Average Alarm Rate
- Maximum (or Peak) Alarm rate
- % of time Alarm rates are outside of acceptability target

The Average alarm rate is defined as a level of acceptability in Table 1 below. EEMUA mentions that the percentage of time alarm rates are outside of the "Very likely to be acceptable" target should be less than 10%.

LONG TERM AVERAGE ALARM RATE IN STEADY STATE OPERATION	ALARM PER OPERATOR		ACCEPTABILITY
	NO. PER HOUR	NO. PER 10 MINUTES	
More than 1 per minute	>60	>10	Very likely to be unacceptable
One per 2 minutes	30	5	Likely to be over-demanding
One per 5 minutes	12	2	Manageable
Less than 1 per 10 minutes	<6	<1	Very likely to be acceptable

Table 1: EEMUA 191 – Benchmark for Assessing Average Alarm Rates

EEMUA shows four levels of acceptability starting with "Very likely to be acceptable" and ending with "Very likely to be unacceptable". In so doing, EEMUA defines a middle range that is not defined in the ISA 18.2 metrics. The EEMUA metric for Manageable is one per 5 minutes. ISA's corresponding metric of ~2 per 10 Minutes is considered by ISA to be the "Maximum Manageable". The EEMUA metrics, therefore, have a bit more granularity for reporting alarm system performance but that granularity is focused on what both standards describe as outside the "Manageable" number of alarms per 10 minutes.

Maximum alarm rates following a plant upset are shown in Table 2. These metrics present a challenge to assess for a couple of reasons. Most software includes Alarm Flood reporting where an alarm system goes into flood when it receives 10 alarms in a 10-minute period and comes out of flood when it drops below five alarms in 10 minutes. Most reporting software focuses on the individual floods, the length of the flood, the number of alarms in the flood, and the peak alarm rate during the flood. However, few focus on the 10 minutes following the flood. Identifying an Upset condition and then assessing the alarm load after the upset, in most cases, requires manual analysis using reports generated by the software to identify upset conditions and then correlate that against the alarm load following the upset. ISA does not have a similar metric

NUMBER OF ALARM DISPLAYED IN 10 MINUTES FOLLOWING A MAJOR PLANT UPSET.	ACCEPTABILITY
More than 100	Definitely excessive and very likely to lead to the operator abandoning use of the system
20 - 100	Hard to cope with
Under 10	Should br manageable - but may be difficult if several of the alarms require a complex operator response.

Table 2: EEMUA 191 – Guidance on Alarm Rate Following an Upset

EEMUA also provides a graphical representation for different levels of performance of an alarm system. A sample scatter graph report for a plant is shown in Figure 6.

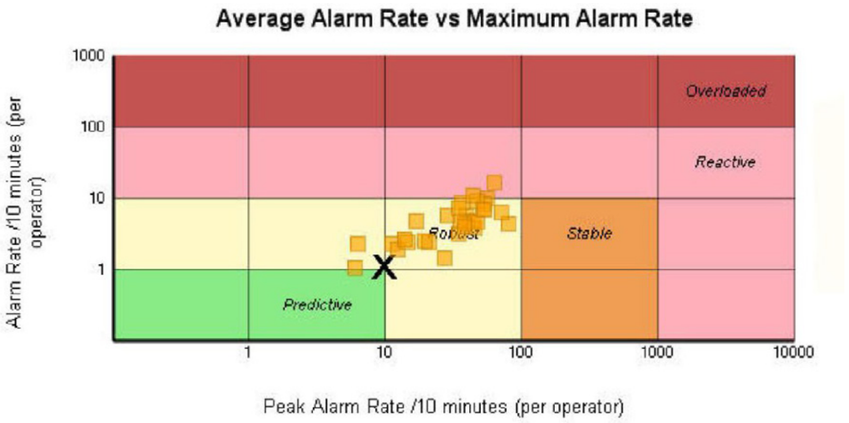


Figure 6: Sample EEMUA Results – Total Plant for One Month

EEMUA also states that a site, which has a control system with greater than 1000 configured alarms, should be targeting fewer than 10 standing alarms and fewer than 30 shelved alarms (excluding maintenance shelved alarms).

ISA 18.2 ALARM PERFORMANCE KPIS

ISA, on the other hand, approaches KPIs a bit differently as can be seen in Table 3. The ISA 18.2 alarm performance metrics and target values are very clearly defined into two categories, “Very Likely to be Acceptable” and “Maximum Manageable”. ISA also places an emphasis on the amount of time spent in various states with specific metrics for the % of time spent in Flood, the % of Hours with more than 30 alarms, and % of 10-minute periods with more than 5 alarms.

It is important, therefore that you understand what these metrics mean. Floods were defined previously but floods are often made up of other bad actor alarms which may or may not represent an upset condition. For example, a chattering alarm is one that alarms and then returns to normal several times in a short period (e.g. 3 times in 1 min). Fleeting and/or momentary alarms turn on and off very quickly (e.g. 10 seconds or less), but do not necessarily repeat. EEMUA defines Standing Alarms as an alarm that comes in and remains in the alarm state for up to 24 hours. ISA 18.2 does not define Standing alarms but both standards agree that Stale alarms are those that go into alarm and do not return to the normal state for 24 hrs or more.

The ISA 18.2 metrics have been adopted as the performance metrics for most of the standards and by most plants. While these targets may initially appear onerous, they are possible over time with continuous effort and plans to monitor and address identified Bad Actor alarms on a regular basis. If your plant’s alarm system performance does not meet the following KPIs, it is important that you can demonstrate continuous improvement with the goal and processes in place to reach these targets.

METRIC	TARGET VALUE	
Annunicated Alarms per Time	Target Value: Very likely to be Acceptable	Target Value: Maximum Manageable
Annunicated Alarms per 10 Minutes per Operating Position	~ 1 (average)	~ 2 (average)
Percentage of hours containing more than 30 alarms	< 1%	
Percentage of 10 minutes periods containing more than 5 alarms	< 1%	
Maximum number of alarms in a 10 minutes period	10 or less	
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 for chattering and fleeting alarms	Zero, action plans to correct any that occur	
State Alarms	Less than 5 present on any day, with action plan 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	
Unauthorised Alarm Suppression	Zero alarm suppressed outside of controlled or approved methodologies	
Improper Alarm Attribute Change	Zero alarm attribute changes outside of approved methodologies or MOC	

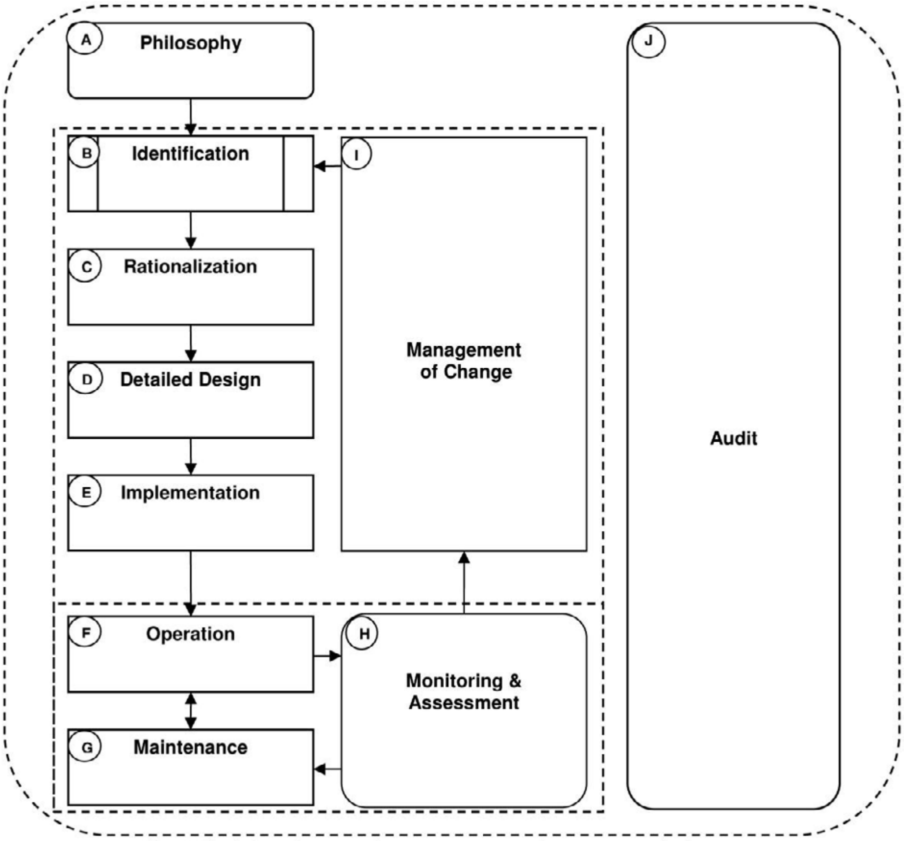
Table 3: Sample ISA 18.2 Alarm Performance KPIs

ISA 18.2 LIFECYCLE MODEL

ISA 18.2 (2009) introduced the lifecycle model (Figure 6) which has since been adopted by every alarm management standard. The lifecycle model defines the alarm system in stages from its specification, through design, and then ongoing operation. Details of each stage are found in the ISA Standard and EEMUA 191 has a section that shows the correlation between chapters in EEMUA 191 and the corresponding ISA 18.2 Lifecycle Model stage.

The lifecycle model is an excellent method of representing the overall process of alarm system management. It is an ongoing process that is suitable for new or existing systems. It has been designed to represent sequential stages, some of which run concurrently with other stages that are linked horizontally (e.g. MOC (Stage I) must be followed by Stages B, C, D, and E).

In some cases, a sequential stage may be "skipped". For example, during a rationalization exercise the outcome may be an alarm setting change, which may not require detailed design to implement. The lifecycle model is, however, limited to computer-based alarm systems and excludes sensors and final control elements. Safety Instrumented Systems (SIS) are also excluded except for any alarms generated from them.



Note 1: The independent stage J represents a process that connects to all other stages.
Note 2: The rounded shapes of stages A, H, and J represent entry points to the lifecycle.

Figure 6: ISA 18.2 Alarm Management Lifecycle

LIFECYCLE MODEL LOOPS

There are three “loops” in the lifecycle model that are represented by the dotted lines in Figure 6. The outer loop includes the Philosophy (Stage A) and Audit (Stage J). Adherence to the Alarm Philosophy and periodic audits of your alarm system are requirements of every standard. The Philosophy controls implementation of the alarm system and the Audit reveals how closely the Philosophy is being followed, the results, and any changes needed.

The next loop could be considered the Implementation loop. It includes Identification, Rationalization, Detailed Design, and Implementation as well as Management of Change as a feedback mechanism (Stages B, C, D, E, and I). This loop takes the concepts and requirements of the Alarm Philosophy and applies them to the development of the alarm system, guiding the process of identifying needed alarms, rationalizing them to ensure proper prioritization, and designing them for operation and presentation. The Management of Change provides a framework to ensure corporate and/or site requirements for managing changes to the site’s hardware and software systems are followed and documented.

The third loop can be considered the Operations loop. If an alarm issue (e.g. chattering alarm) is detected in Monitoring and Assessment (Stage H), it would most likely be resolved within the Operations loop by normal Maintenance (Stage G). However, a more complex issue that required an MOC would require the issue flow back through the Implementation loop to ensure any required changes meet the standards set within that loop. Maintenance for simple issues is typically resolved within the Operations loop whereas issues which result in any design changes that require Management of Change are referred back to the Implementation loop to ensure they meet the standards set within that loop.

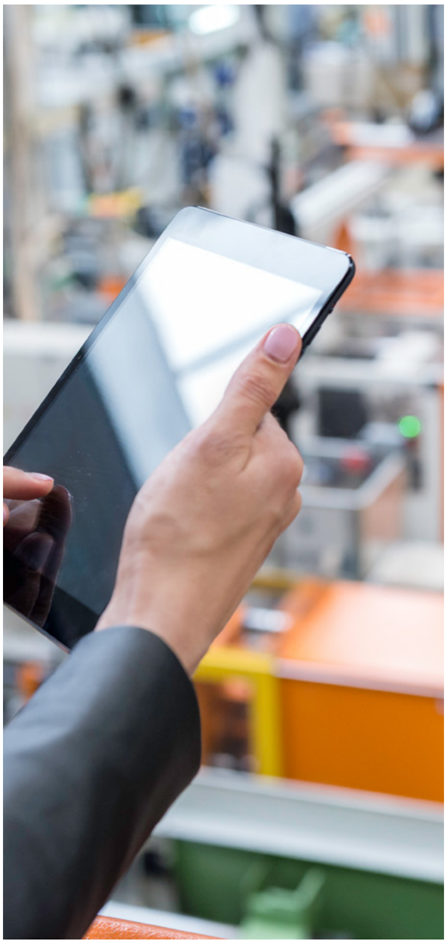
STAGES OF THE LIFECYCLE MODEL

PHILOSOPHY

An Alarm Philosophy (Stage A) documents the site’s approach to alarm management and is a mandatory requirement. It includes the definitions, principles and details of the practices and procedures for each of the remaining life cycle stages. It further defines the configuration for reporting bad actor alarms like chattering, fleeting and floods as well as guidelines for shelving and suppression and the necessary consequences, severities, response times and alarm priority matrix needed for Alarm Rationalization. The Alarm Philosophy provides a lasting reference to sustain an effective alarm system. Both ISA 18.2 and EEMUA 191 include a table containing the required and recommended contents of the Alarm Philosophy.

IDENTIFICATION

Many methods are available to determine if an alarm is required. The Identification (Stage B) may use some of these such as; Process Hazard Analysis (PHA), incident investigations, HAZOPS/CHAZOPS, and alarm design/rationalization workshops. The outcome of a HAZOP might be that an alarm is required to warn the operator of an abnormal situation (e.g. High Pressure). Typically, however, a HAZOP exercise does not consider the following; is the tag the most suitable indication of the condition to alarm, what is the ideal setting, configuration details, the potential operator workload etc. These details are discussed in the Rationalization stage before an alarm is to be implemented. The Identification stage and the following three stages are closely related, however, due to different terminology used in the various process industries, it can be somewhat confusing as to which steps in the overall design process are undertaken in each stage.



RATIONALIZATION

Alarm Rationalization (Stage C) is about reconciling each individual alarm against the principles and requirements of the alarm philosophy. It is important that the relevant data for each alarm is documented to support the other stages of the life cycle. This includes the alarm description, settings, causes of an alarm, the consequence of no action, the required operator action, amount of time available for the operator to respond, severity of consequence if no action is taken, etc. The severity of the consequences and the response time are documented, and the alarm priority is determined from an Alarm Priority Matrix based on the severity of consequences and the response time. This matrix is defined in the alarm philosophy.

DETAILED DESIGN

The design phase (Stage D) includes the basic DCS/PLC configuration of the alarm, Human Machine Interface (HMI) for the alarm, and any advanced methods of alarm management. These requirements should be documented in the Alarm Philosophy and some may be determined during the rationalization process.

IMPLEMENTATION & TRAINING

The Implementation stage (Stage E) involves the various other activities required to put the alarm into service. It includes testing of the alarm system functions as well as relevant training for the operators and other personnel.

OPERATION

Operation (Stage F) is the beginning of a three-stage continuous improvement loop that ensures the alarm system continues to operate optimally. The alarm is now in service and reporting abnormal conditions to the operator.

MAINTENANCE

Maintenance (Stage G) is an essential stage that must be addressed and planned for in this continuous improvement loop. Process measurement instruments, final control elements, and control systems all require periodic/predictive maintenance to ensure their continued reliable operation. This is critical to ensure the ongoing performance of the alarm system.

MONITORING & ASSESSMENT

Monitoring & Assessment (Stage H) includes the periodic collection and analysis of data from alarms. Without monitoring it is virtually impossible to maintain an effective alarm system. Assessment, typically in the form of alarm system reports, should be undertaken frequently (daily or weekly) and is the primary method for determining problems such as nuisance alarms, stale alarms, and alarm floods, and developing action plans to address the issues.

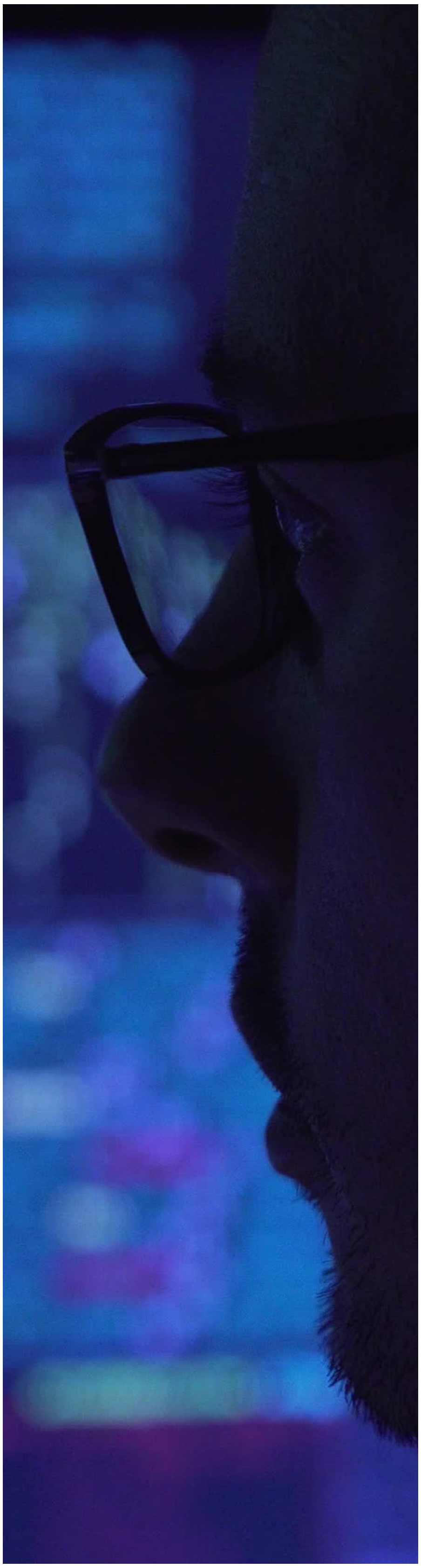
MANAGEMENT OF CHANGE

Management of Change (Stage I) is a critical stage that helps ensure the ongoing integrity of the alarm system. During routine maintenance or from the monitoring and assessment of the alarms system and identification of nuisance alarms, it is often required that activities follow the site's formal MOC process. This needs to be a structured process of approval and authorization for any additions, modifications, and deletions of alarms from the system. The results of an MOC change to the Alarm System may require other stages of the system be reviewed to ensure the change does not impact Identification, Rationalization, Design, or Implementation.

AUDIT

A periodic Audit (Stage J) of the alarm system and the processes detailed in the alarm philosophy may determine the need to modify processes, the philosophy, or the design etc. Every standard includes a requirement for periodic, regularly scheduled Audits either by direct mention or by reference to ISA 18.2 or EEMUA 191. Some of these include additional requirements around audits. For example; DOT / PHMSA 2009 standard includes specific time frames for certain audit activities like auditing inhibited alarms monthly and a complete audit of the alarm system once per year. Certain Alarm Classes, as defined in the site's Alarm Philosophy, may also carry an auditing requirement such as alarms associated with safety systems.

Care should be taken about audit requirements documented or included in the Alarm Philosophy to ensure that requirements are met without exception. The audit may also reveal that an organization's discipline to follow the processes (especially MOC) needs improvement. In the event of an accident resulting in injuries or environmental damage, litigants may require proof that audits were conducted per schedule and measures were taken to address any shortcomings identified in the audit.



WHAT STEPS CAN YOU TAKE TO COMPLY?

Now is the time to act. The following steps will help you get on the road to compliance:

- Purchase ISA 18.2 and/or EEMUA 191.
- Undertake some form of an audit of your alarm system. An audit will highlight the current alarm system performance and help you identify deficiencies of your alarm system and the areas that need to be improved. As an absolute minimum, undertake a benchmarking and assessment project to determine if your alarm rates are acceptable. Benchmarking also provides a point of reference to help measure improvements achieved through implementing an Alarm Management Program that conforms to the standards.
- It is critical to get senior management sponsorship for an alarm system improvement project. Information that should help management sponsor your project are operator survey results, a Bad Actor analysis report, and/or the audit/benchmarking results which compares your plant alarm system KPIs with ISA 18.2 and EEMUA 191 requirements.
- Prepare a Strategic Plan to reach compliance. This plan may contain the following:
  - Alarm Philosophy Document Development and then Functional Specifications.
  - Purchase of alarm database and associated software tools.
  - Identify and rationalize Top 20 most frequent alarms and/or Classic rationalization of all alarms depending on budget and the state of the alarm system.
  - Project plan for the next 12 – 24 months (including milestones).
  - Required training – engineers, technician, and operators.
- Implement the Strategic Plan

Honeywell offers a full range of software and services to assist you at every stage of this process. Contact your account manager or go to (https://www.honeywellprocess.com/en-US/online_campaigns/alarm-management/Pages/alarm-management.html#home) for more information.

CONCLUSION

> **As more scrutiny has been placed on Alarm Management many plants have embarked on alarm management projects to satisfy insurance companies, investors, or other regulatory bodies.**

Through many visits to numerous processing plants, however, the situation remains that many plants are still not taking alarm management seriously enough. What has been noted in some cases is an effort to satisfy the requirement in name only rather than implement a robust alarm management program with an eye on the benefits such a program can provide.

The Alarm System is an essential part of your plant's Layers of Protection and as such should be implemented and maintained to the levels stated in ISA 18.2 and EEMUA 191. A well implemented Alarm Management program can deliver results that not only improves the operator's situational awareness, decreases the potential of a safety related incident, and enhances environmental compliance but also reduces unplanned downtime, helps prevent equipment damage, lessens production losses due to off-spec production, and improves overall plant profitability.

References

- ANSI/ISA-18.2-2016 "Management of Alarm Systems for the Process Industries".
- EEMUA Publication 191 Edition 3 (2013) "ALARM SYSTEMS - Guide to Design, Management, and Procurement".
- IEC 62682 (2014) "Management of Alarm Systems for the Process Industries".

For more information

Learn more about how Honeywell's alarm management solution can improve safety and reliability at your plant, visit our website, www.honeywellprocess.com/software or contact your Honeywell account manager.

Contact Us:

715 Peachtree St NE
Atlanta GA 30308
1 (877) 841-2840

www.honeywell.com

THE
FUTURE
IS
WHAT
WE
MAKE IT

Honeywell