OCTAVE

WHITE PAPER

Understanding and applying the ANSI-ISA 18-2 alarm management standard

Contents

Abstract

Alarm management has become an ever-increasing topic of discussion in the power and processing industries. In 2003, ISA started developing a standard around this subject. The first version of that standard, ANSI/ISA-18.2-2009 Management of Alarm Systems for the Process Industries was published in 2009. ISA periodically updates and reviews its standards, and in 2016 an updated version of 18.2 was issued. The differences were minor.

This paper reviews the scope, regulatory impact, requirements, recommendations, alarm definitions and other details of the standard.

Overview

In the mid-1990s, alarm management became an important topic in the process industries. The alarm problem and its solution became the subject of several articles and technical symposia reports.

In 2003, ISA began developing an alarm management standard. Dozens of contributors from various industry segments spent thousands of hours participating in the development. Prior to being acquired by Octave, PAS participated as both a section editor and a voting member. After six years of work, the original ANSI/ISA-18.2-2009 Management of Alarm Systems for the Process Industries (ISA-18.2) standard was released.

The issuance of ISA-18.2 was a significant event for the chemical, petrochemical, refining, power generation, pipeline, mining and metals, pharmaceutical and similar industries using modern control systems with alarm functionality. It sets forth the work processes for designing, implementing, operating and maintaining a modern alarm system in a lifecycle format. It also has a considerable regulatory impact.

ISA-18.2 is quite different from the usual ISA standard. It is not about specifying communication protocols between equipment or the detailed design of control components. It is about the work processes of people. Alarm management is not really about hardware or software; it is about work processes. Poorly performing alarm systems do not create themselves. ISA-18.2 is a comprehensive standard developed per stringent methods based on openness, balancing of interests, due process and consensus. These components make it a recognized and generally accepted good engineering practice from a regulatory point of view.

ISA works closely with the International Electrotechnical Commission (IEC). The IEC is the standards-making body for the World Trade Organization (WTO). In process control, the ISA originates standards and the IEC then reviews, modifies and adopts them for use by WTO member countries. This process took place for ISA 18.2-2009, resulting in the issuance of IEC-62682 v1.0 in 2014. In general, the IEC makes few technical changes to such ISA standards but does tend to make some things mandatory (shall) that ISA documents characterize as recommended (should).

After the issuance of IEC 62682 v1.0, the ISA updated 18.2 to a 2016 version. IEC 62682 continues to evolve through periodic updates, maintaining alignment with ISA-18.2. Ongoing enhancements are being delivered through new and updated technical reports and working group initiatives ISA standards are available at www.isa.org.

This white paper will review the most important aspects of the scope, requirements, recommendations and other contents of ISA-18.2. However, there is no substitute for obtaining and understanding the full document.

1. Purpose and scope

The basic intent of ISA-18.2 is to improve safety. Ineffective alarm systems have often been documented as contributing factors to major process accidents. The alarm system problems that ISA-18.2 addresses have been well-known for almost three decades.

There are several common misconceptions about standards. Standards intentionally describe the minimum acceptable and not the optimum. By design, they focus on the “what to do” rather than the “how to do it.” By design, standards do not have detailed or specific “how-to” guidance. ISA-18.2 does not contain examples of specific proven methodologies or detailed practices. The standard focuses on both work process requirements (shall) and recommendations (should) for effective alarm management.

Standards have significant importance compared to articles, reports, books or guidelines. Standards are developed in accordance with stringent American National Standards Institute (ANSI) methodologies. As such, regulatory agencies regard ISA standards as recognized and generally accepted good engineering practice (RAGAGEP). This means that such agencies can and have used standards as the basis for enforcement actions, including penalties.

ISA issues technical reports for the purpose of explaining a standard and providing examples. Technical reports have no mandatory content. There is more information on seven different ISA alarm management technical reports later in this document.

2. Does ISA-18.2 apply to you?

The focus of ISA-18.2 is on alarm systems that are part of modern control systems, such as distributed control system (DCS), SCADA systems, programmable logic controllers (PLCs) or safety systems. It applies to plants with operators responding to alarms depicted on a computer-type screen and an annunciator.

This includes the bulk of all processes operating today, specifically:

- Chemical
- Refining
- Platform
- Pipelines
- Power plants
- Pharmaceuticals
- Mining and metals

Additionally, it applies whether your process is continuous, batch, semi-batch or discrete. The reason for this commonality is that alarm response is not a function of the specific process being controlled; it is a human-machine interaction. The steps for detecting an alarm, analyzing the situation and reacting are performed by the operator. There is little difference if you are making (or moving) gasoline, plastics, megawatts or aspirin. While many industries feel "we're different," that is not the case regarding alarm response. Many different industries participated in the development of ISA-18.2, recognized this, and the resulting standard has overlapping applicability.

ISA-18.2 indicates the boundaries of the alarm system relative to terms used in other standards, such as Basic Process Control System (BPCS), Safety Instrumented System (SIS), etc. Several exclusions are listed to not contradict existing content in other standards.

3. Regulatory impact

This paper is not intended to be a detailed clause-by-clause interpretation of Occupational Safety and Health Administration (OSHA), Environmental Protection Agency (EPA), Department of Transportation (DOT) and Pipeline and Hazardous Materials Safety Administration (PHMSA) or other regulations. The regulatory environment is complex and overlapping for some industry segments.

For example, many US industries are clearly covered by OSHA 1910.119 Process Safety Management, which makes a few specific mentions of alarms.

Regulatory agencies often have general duty clauses and interpretations. For example, OSHA 1910.119 (d)(3) (ii) states, the employer shall document that equipment complies with recognized and generally accepted good engineering practices, (RAGAGEP).

Codes, standards and practices are usually considered recognized and generally accepted good engineering practices. The OSHA interpretation letter to ISA states that a National Consensus Standard, such as ISA-18.2, is a RAGAGEP. OSHA similarly recognizes ANSI/ISA S84.01-1996 as an example. A memorandum of understanding exists between OSHA and ANSI regarding these matters.

Generally, a regulated industry can be expected to either comply with RAGAGEP or explain and show they are doing something just as good or better. Indeed, OSHA sought and received permission from ISA to internally distribute ISA-18.2 to its inspectors. This was with the specific intent to be able to easily cite it in investigations and use it for enforcement reasons.

4. Grandfathering

A grandfather clause used by other ANSI/ISA standards was also used in ISA-18.2. It is:

> “For existing alarm systems designed and constructed in accordance withcodes, standards and/or practices prior to the issue of this standard, the owner operator shall determine that the equipment is designed, maintained, inspected, tested and operated in a safe manner. The practices and procedures of this standard shall be applied to existing systems in a reasonable time as determined by the owner operator.”

The two instances of “shall,” which are highlighted, indicate mandatory requirements. This clause mimics language used in OSHA regulation 1910.119(d)(3)(iii).

5. Definitions in ISA-18.2

Much work was done researching and carefully crafting various definitions while maintaining consistency between ISA-18.2 and other references.

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.”

6. Alarm state transitions

ISA-18.2 includes a moderately complex diagram depicting the alarm states and sub-states of “normal,” “unacknowledged,” “acknowledged” and “returned-to-normal.” Of particular interest are the states of “shelved,” “suppressed by design” and “out-of-service.” These have specific meanings:

“Shelved” is an alarm that is temporarily suppressed, usually via a manual initiation by the operator, using a method meeting a variety of administrative requirements to ensure the shelved status is known and tracked.

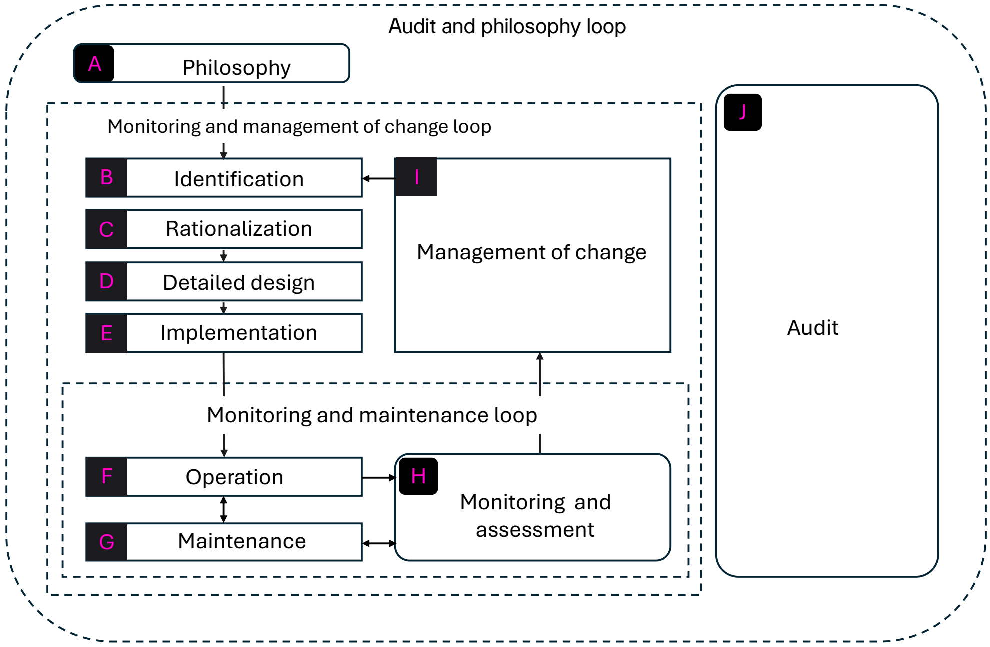
“Suppressed by design” is an alarm intentionally suppressed by a designed condition. This is a generic description that includes such items as simple logic-based alarms and advanced state-based alarming techniques.

“Out-of-service” is a non-functioning alarm, usually for reasons associated with the maintenance stage of the lifecycle. An “out of service” alarm is also tracked via similar administrative requirements to a shelved alarm.

The terms suppress and alarm suppression are intentionally generic and not specific to a type of DCS. They indicate when the alarm functionality is not working (generally through an override mechanism of some sort). It is possible, and unfortunately common, to suppress an alarm outside of the proper work practices, and detecting such undesirable situations is part of the monitoring lifecycle stage .

7. The alarm management lifecycle

ISA-18.2 is written with a lifecycle structure comprised of 10 stages. In this figure from 18.2-2016, they are:



Note

1 The box used for stage B represents a process defined outside of this standard per 5.2.2.3.
2 The independent stage J represents a process that connects to all other stages per 5.2.2.11.
3 The rounded shapes of stages A, H, and J represent entry points to the lifecycle per 5.2.3.
4 The dotted lines represent the loops in the lifecycle per 5.2.5.

Alarm philosophy: Documents the objectives of the alarm system and the work processes to meet those objectives.

Identification: Work processes determining which alarms are necessary.

Rationalization: The process of ensuring an alarm meets the requirements outlined in alarm philosophy, including the tasks of prioritization, classification, settings determination and documentation.

Detailed design: The process of designing the aspects of the alarm to meet the requirements determined in rationalization and in the philosophy. This includes some HMI depiction decisions and can include the use of special or advanced techniques.

Implementation: The alarm design is brought into operational status. This may involve commissioning, testing and training activities.

Operation: The alarm is functional. This stage includes refresher training if required.

Maintenance: The alarm is non-functional because of either test or repair activities. Do not equate this lifecycle stage with the maintenance department or function.

Monitoring and assessment: The alarm system's performance is continuously monitored and reported against the goals in the alarm philosophy.

Management of change: Changes to the alarm system follow a defined process.

Audit: Periodic reviews are conducted to maintain the integrity of the alarm system and alarm management work processes.

7.1. Lifecycle stages vs. activities

Do not confuse a lifecycle stage with an activity. Lifecycle is a structure for the content of the ISA-18.2 document. It is not specifically or necessarily a list of activities to be accomplished in a particular order.

For example, in a matter of minutes, an engineer could sit down and resolve a single nuisance chattering alarm. That task could involve going through several different lifecycle stages as part of performing the activities associated with a simple task. Consider the following:

Monitoring stage: Engineer: "Well, today, I am spending some time fixing nuisance alarms. Which of my alarms are on the most frequent alarm list? Ah, there's one – a chattering high-value alarm on the column pressure."

Identification stage: Engineer: "Yes, I happen to remember that we need this alarm as part of our quality program; however, my job today is to make it work correctly and eliminate the chattering behavior, not to decide whether to get rid of it or not. So I don't have to research whether it was originally specified by some particular process like a process hazard analysis (PHA)."

Detailed design stage: Engineer: "Let's check the configuration of this alarm. There's nothing unusual about it. Hmmm, I see that the alarm deadband on this point is set to zero. That's certainly not proper and could easily lead to chattering behavior. Let's examine some process history and alarm history and consult a good book on alarm management to determine a more appropriate deadband setting."

Operation stage and maintenance stage: Engineer: "Now I am going to alter the alarm deadband to a new setting. Hmmm, do I have to take the point off-scan to do that? Not in this case, on this DCS. If I did, I would have to tell the operator first. But I can make this change without that and the alarm will remain online throughout."

Management of change stage: Engineer: "So far, I haven't actually changed anything. Before I type in and activate this new number for deadband, I mentally review the management of change requirements for doing so. This specific type of change is covered in our alarm philosophy, and our site procedures empower me to make this change as part of my authorized job duties. I do not have to seek any approval or signatures. I will have to document this change in the master alarm database though."

Implementation stage: Engineer: "Now I actually change the deadband. I type in the new number and hit 'enter.' Done."

Rationalization stage (which includes alarm documentation): Engineer: "Since I have the proper security access, I will add this new deadband setting into the master alarm database along with my name, date and reason. I will also make a note in the weekly nuisance alarm tracking report about this one. As long as I am here looking at this alarm, I note it is configured as a priority three. That seems reasonable, but let's just check the online master alarm database for the factors that resulted in the priority assignment. Hmmm, they look pretty good. If they did not, I could not change them myself. I would need the prioritization team to take a look at it. Any change in priority requires notification to the operators."

Monitoring stage: Engineer: "Part of my work process for this is to continue to look at the alarm data to see if this deadband setting change solved the problem. I will add this one to my tracking and follow-up list."

In a few minutes, several different lifecycle stages were briefly visited in accomplishing this one example task. In understanding and applying ISA-18.2, do not get overly concerned about trying to figure out which lifecycle stage you are in at any point in time. It is a requirements structure, not a work process sequential checklist.

Octave published *The Alarm Management Handbook,* which provided a proven seven-step methodology for solving an alarm system problem and accomplishing effective alarm management. There is no conflict between this seven-step approach and the ISA-18.2 lifecycle methodology; there is only some different nomenclature and task arrangement. The original edition of the Handbook predated the release of ISA-18.2, but the Second Edition contains full coverage and explanation of that standard.

8. The alarm philosophy lifecycle stag

ISA-18.2 recognizes that an alarm philosophy document is a key requirement foreffective alarm management. A table lists topics notes as mandatory or recommended for inclusion. Remember that a standard describes the minimum acceptable, not the optimum.

The major mandatory contents of the alarm philosophy include roles and responsibilities, alarm definition, the basis for alarm prioritization, HMI guidance, performance monitoring, management of change and training.

There are no surprises in the list except for two concepts not previously included in the alarm management lexicon, alarm classification and highly managed alarms.

8.1. Alarm classification

Alarm classification is a method for assigning and keeping track of various requirements for alarms, mostly administrative ones. For example, some alarms may require periodic refresher training, while others may not. The same could be true for testing, maintenance, reporting, HMI depiction and similar aspects. Alarm classes are defined and used to keep track of these requirements. It is mandatory in ISA-18.2 to define alarm classes.

This is a slightly unusual thing for a standard. Normally, standards tell you what to do but not how to do it, or to require a specific method. For example, the standard could have simply stated, "Identify and track alarms that require periodic testing." There are various methods to successfully do this, and a classification structure is only one of them. However, the committee elected to require a classification structure, though it need not be an onerous one. No specific class requirements and no minimum number of class definitions are specified. Octave recommends the "keep it simple" approach and has a straightforward class structure with minimal variations.

8.2. Highly managed alarms

The committee thought it desirable to explicitly define one class of alarms. A variety of designations were considered, from critical to vital to special to super-duper. Highly managed alarms (HMAs) was chosen as the term. The intent is to identify the alarms that must have a considerably high level of administrative requirements. ISA 18.2 lists over 30 requirements for alarms designated as HMAs.

Now, there is no requirement to have or use this classification. However, if you state, "this classification in my philosophy is per the ISA-18.2 usage of highly managed," you must document and handle that multitude of special administrative requirements precisely according to the standard. The various mandatory requirements for HMAs are spread over several sections throughout ISA-18.2.

This includes:

- Specific shelving requirements, such as access control with audit trail
- Specific out of service alarm requirements, such as interim protection, access control and audit trail
- Mandatory initial and refresher training with specific content and documentation
- Mandatory initial and periodic testing with specific documentation
- Mandatory training around maintenance requirements with specific documentation
- Mandatory audit requirements

Octave's advice is to specifically avoid the usage of this alarm classification. You might choose a similar classification and then select only the administrative requirements necessary for those alarms. These will probably be only a subset of the ISA-18.2 listing for HMAs.

9. The alarm systems requirements specification (ASRS)

This non-mandatory section says that if you buy a new control system, it is a good idea to write down your requirements and evaluate vendor offerings and capabilities against them. Specific deficiencies in the chosen system can drive the acquisition or creation of third-party or custom solutions. The ASRS then becomes a useful document for system testing and acceptance.

10. The alarm identification lifecycle stage

This section of ISA-18.2 notes that different methods are used to initially identify the need for some alarms. All modern control systems have a lot of built-in alarm capability; perhaps more than a dozen types of alarms available for some point types.

In some cases, the need to use one of those types or create a specific alarm via custom logic or calculation may be driven from various process-related sources. These are the usual list of studies such as a PHA, layer of protection analysis (LOPA) and failure mode and effects analysis (FMEA).

11. The alarm rationalization lifecycle stage

This lifecycle stage consists of several activities. Most people familiar with alarm management concepts think of rationalization as the specific activity of a team reviewing an alarm system and making decisions about usage, priority and setpoints. In ISA-18.2, the word is used to indicate a collection of activities that may be done in various ways. The activities are as follows:

- Ensuring alarms meet the criteria set forward in the alarm philosophy
- Justifying the need for the alarm
- Marking for deletion alarms that should not exist
- Determining the appropriate alarm type
- Determining the appropriate alarm setpoint or logical condition
- Determining the proper priority
- Documenting any special design considerations for an alarm
- Documenting any advanced alarming capabilities desired for an alarm
- Documenting relevant information such as operator action and consequences
- Determining the alarm's classification

Note that all of the activities listed above include both the review of already existing alarms or consideration of potential new alarms. The major mandatory contents of the rationalization stage are for specific alarm documentation and alarm classification.

The section is quite short since it intentionally avoids listing specific methods for effective and efficient rationalization.

12. The basic alarm design lifecycle stage

This section describes the common capabilities of control system alarm functionality and how they relate to the alarm state diagram. There is some non-mandatory advice about the proper usage of some alarm types and some alarm configuration capabilities, such as deadband and delay time.

13. Human-machine interface (HMI) design for alarm systems

This section describes the desired functionality for indicating alarms to the operator. ISA 18.2 is designed not to overlap content in the ISA-101 standard on human-machine interfaces.

Some items discussed (with little detail), include:

- Depiction of alarm states, priorities and types
- Alarm silencing and acknowledgment
- Alarm shelving, designed suppression and out-of-service conditions and depiction
- Alarm summary display functionality
- Other alarm-related similar displays and functionality
- Alarm sounds
- Alarm information and messages
- Alarm annunciators

Note that all of the activities listed above include the review of already existing alarms or consideration of many functionality items listed as mandatory or recommended. The major mandatory items are for specific depiction of various alarm-related conditions and specifically required HMI screens and functionality. These items are typically within the capabilities of most modern control systems. At the start of the section, it is noted that some described features are not possible in some control systems. You can still comply with the standard if you have such a system.

The ISA-101 HMI standard contains basic principles but very little detail and few examples. For more detailed information on creating proper and effective operator graphics, we recommend Octave's book, *The High Performance HMI handbook*, and the two-part follow-up white papers that greatly expand it with additional examples and case studies. Those papers also provide detailed explanation of the ISA-101 standard.

14. Enhanced and advanced alarm methods

This is an informative section providing an overview of alarm features and capabilities that are usually a bit beyond the standard capability of a control system. This section notes that usage of such advanced capabilities may require additional design work and support.

These types of advanced methods briefly discussed include the following

- Information linking
- Logic-based alarming
- Model-based alarming
- Alarm attribute modification
- Externally enabled systems
- Logical alarm suppression/attribute modifications
- State-based alarming
- Model-based alarming
- Non-control room considerations (such as remote alarm notifications)
- Paging, e-mailing and remote alerting systems
- Supplementary alarm systems
- Continuously variable alarm thresholds
- Batch process alarm considerations
- Training, testing and auditing systems
- Alarm attribute enforcement

15. The implementation lifecycle stage

This section covers the activities and requirements around implementing a new alarm system or implementing desired changes to an existing one. The areas covered generally have both mandatory requirements and non-mandatory recommendations.

They are as follows:

- Planning
- Training for new systems and modifications
- Testing and validation for new systems and modifications
- Documentation of training and testing

16. The operation lifecycle stage

This section deals with mandatory requirements and non-mandatory recommendations for in-service and operating alarms. The areas addressed are:

- Alarm response procedures
- Alarm shelving, including documentation
- Operator refresher training, including documentation

17. The maintenance lifecycle stage

This section is not about the maintenance department or the maintenance function. It is about the condition where an alarm has been removed from service specifically for testing or repair. The section covers mandatory requirements and non-mandatory recommendations for the following:

- Moving alarms in and out of the maintenance stage of the lifecycle, including notification, tracking and documentation
- Interim procedures for when alarms are out of service
- Periodic testing of alarms, including record-keeping
- Refresher training for personnel involved with alarm repair or testing
- Alarm validation regarding equipment replacement

18. The monitoring and assessment lifecycle stage

This is the stage in which alarm system performance is measured and reported. The intent is to verify that the other lifecycle stages successfully create an effective alarm system.

It is mandatory that alarm system performance be measured and compared against goals identified in the alarm philosophy. Four clearly defined terms are used in this section: monitoring, assessment, audit and benchmark.

Several analyses are described and recommended for alarm system performance measurement. A non-mandatory table indicating recommended performance goals and metrics is provided in 18.2-2016 as Table 7. The numbers allow for possible modifications, and are preceded by the following statement:

> “The target metrics described below are approximate and depend upon many factors (process type, operator skill, HMI, degree of automation, operating environment, types and significance of the alarms produced). Maximum acceptable numbers could be significantly lower or perhaps slightly higher depending upon these factors. Alarm rate alone is not an indicator of acceptability.”

Alarm performance metrics based upon at least 30 days of data		
Metric	**Target value**	
Annunciated alarms per time	Target value: very likely to be acceptable	Target value: maximum manageable
Annunciated alarms per hour per operator console	~6 (average)	~12 (average)
Annunciated alarms per 10 minutes per operator console	~1 (average)	~2 (average)
Metric	**Target value**	
Percentage of 10-minute periods containing more than 10 alarms	~<1%	
Maximum number of alarms in a 10-minute period	≤10	
Percentage of time the alarm system is in a flood condition	~<1%	
Percentage contribution of the top 10 most frequent alarms to the overall alarm load	~<1% to 5% maximum, with action plans to address deficiencies.	
Quantity of chattering and fleeting alarms	Zero, 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)	

Table 7: Recommended alarm performance metrics summary

The analyses described are:

- Average annunciated alarm rate per operating position (per hour, per 10 minutes, with acceptability numbers)
- Peak annunciated alarm rates per operating position
- Alarm floods (calculation methods and recommendations)
- Frequently occurring alarms
- Chattering and fleeting alarms
- Stale alarms
- Annunciated alarm priority distribution (alarm occurrences)

The committee researched to achieve consensus in deciding the particular measures and performance numbers. Several analyses with problematic concerns were intentionally left out. Recommendations for the reporting of alarm system analyses are provided.

19. The management of change lifecycle stage

This section deals with mandatory requirements and non-mandatory recommendations for change of the alarm system.

The items covered are:

- Changes subject to management of change
- Change review process requirements, including the consideration of technical basis, impact, procedure and documentation modifications, review and authorization

- Ensuring changes are in accordance with the alarm philosophy
- Temporary changes
- Implementation of changes
- Change documentation requirements and recommendations
- Alarm decommissioning recommendations
- Alarm attribute modification requirements and recommendations

20. The audit lifecycle stage

The audit stage involves a more comprehensive review of not only the performance of the alarm system itself, but also of the various work processes associated with it. The section covers the nature of audits, items to be examined and some recommendations around practices, such as interviews and action plans.

21. ISA technical reports associated with ISA-18.2

The content of a standard is intentionally constrained. Specific methods to accomplish requirements are not provided and examples are limited. Informative content in a standard is kept to a minimum. Much of the content specifically excluded from a standard is exactly what the reader needs to become compliant with the standard. For that reason, ISA develops and publishes technical reports (TRs).

TRs contain:

- Informative material to explain how to apply a standard.
- Examples, alternatives and "how to" information, clearly marked as such. All of those must also be proven in practice and be "recognized and generally accepted." Examples are vendor or product-neutral.
- Proven methods based on real-world experience.
- Work processes with alternatives that have been shown to be successful. A TR does not contain new ideas that have not been tried but might work.

Since the issue of ISA 18.2, seven TRs expanding on its contents have been published. These are:

- ISA 18.2 TR1: Alarm Philosophy Document
- ISA 18.2 TR2: Alarm Identification and Rationalization
- ISA 18.2 TR3: Basic Alarm Design
- ISA 18.2 TR4: Enhanced and Advanced Alarm Methods
- ISA 18.2 TR5: Alarm System Monitoring, Assessment and Auditing
- ISA 18.2 TR6: Alarm Systems for Batch and Discrete Processes
- ISA 18.2 TR7: Alarm Management When Utilizing Packaged Systems

These technical reports are useful resources. All the topics in ISA 18.2 Technical Reports 1 through 5 are covered in considerably more detail and with much more real-world, practical and proven advice, in *The Alarm Management Handbook*, Second Edition.

The *Handbook* has entire chapters on

- Alarm rationalization with cost-effective techniques
- Nuisance alarm resolution
- Alarm performance monitoring
- Advanced techniques, human factors issues and several other topics
- Full coverage of ISA-18.2

The *Handbook* is based on experience from hundreds of successful alarm improvement projects and terabytes of real-world alarm data.

Summary

ISA-18.2 (and the IEC 62682 version) are important standards with worldwide applicability. It has had widespread adoption since the original issue date of 2009. The regulatory issues associated with it are significant. All companies with process control systems that use alarm functionality for operators must be familiar with this standard.

About the author

Bill R. Hollifield

Principal process safety consultant

Bill is a retired principal consultant who was responsible for the areas of both alarm management and high performance HMI. He is a member of the ISA SP-18 Alarm Management Committee, the ISA-SP101 HMI Committee, The American Petroleum Institute's API RP-1167 Alarm Management Recommended Practice Committee and the Engineering Equipment and Materials Users Association (EEMUA) Industry Review Group.

Bill has multi-company, international experience in all aspects of alarm management and HMI development. He has 28 years of experience in the petrochemical industry in engineering and operations and an additional 18 years in alarm management and HMI software and services for the petrochemical, power generation, pipeline, pharmaceutical and mining industries.

Bill is co-author of *The Alarm Management Handbook, The High Performance HMI Handbook* and *The Electric Power Research Institute (EPRI) Guidelines on Alarm Management for both Power Generation* and *Power Transmission.*

Bill has authored several papers on Alarm Management and HMI and is a regular presenter on such topics in such venues as API, ISA, and Electric Power symposiums. He has a BSME from Louisiana Tech University and an MBA from the University of Houston.

In 2014, Bill was made an ISA Fellow.

About Octave

Octave is a leader in enterprise software, turning data into decisive action and intelligence into your edge. Our software solves for and simplifies complexity, from the design and build to operations and protection of people, property, and assets– for any scope, at any scale. For decades, we've partnered with customers to sharpen performance, elevate efficiency, and amplify results. From factory floors to entire cities, our solutions are tuned to scale up what's possible from day one onward.