Understanding and Applying the ANSI/ ISA 18.2 Alarm Management Standard

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. After six years of hard work, the ANSI/ISA-18.2-2009 Management of Alarm Systems for the Process Industries standard was published. This paper reviews the scope, regulatory impact, requirements, recommendations, alarm definitions, and other details of the standard.

Overview

Over the last several years, alarm management has become a highly important topic, and the subject of a number of articles, technical symposia, and books.

In 2003, ISA began developing an alarm management standard. Dozens of contributors, from a variety of industry segments, spent thousands of hours participating in the development. PAS participated as both a section editor and a voting member. After six years of work, the new ANSI/ISA-18.2-2009 Management of Alarm Systems for the Process Industries (ISA-18.2) standard was released. It is available at www.isa.org.

The issuance of ISA-18.2 is 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 life cycle format. It will also have considerable regulatory impact.

ISA-18.2 is quite different from the *usual* ISA standard. It is not about specifying communication protocols between equipment, nor 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.

In this white paper, we 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 nearly two 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 of detailed practices. The standard focuses on both work process requirements ("shall") and recommendations ("should") for effective alarm management.

Readers familiar with alarm management literature should not expect to learn new or different information when reading the ISA-18.2. The key difference is that ISA-18.2 is a **standard**, not a guideline or a recommended practice, and it was developed in accordance with stringent ANSI methodologies. As such, it will be regarded as a "recognized and generally accepted good engineering practice" (RAGAGEP) by regulatory agencies. ISA-18.2 is in the process of being adopted as an International IEC standard (IEC 62682 Ed. 1.0)[1].

The ISA-18.2 committee is now working on creating additional explanatory and methodology information in follow-up ISA technical reports. These should be available in 2011.

1. See http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=e&wwwprog=pro-det.p&progdb=db1&He=IEC&Pu=62682&Pa=&Se=&Am=&Fr=&TR=&Ed=1.0

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 DCSs, SCADA systems, PLCs, or Safety Systems. It applies to plants with operators responding to alarms depicted on a computer-type screen and/or an annunciator.

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

- Petrochemical
- Chemical
- Refining
- Platform
- Pipelines
- Power Plants
- Pharmaceuticals
- Mining & Metals

Additionally, it applies whether your process is continuous, batch, semi-batch, or discrete. The reason for this commonality is that alarm response is really 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 steps 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 simply not the case when it comes to 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 intending to be a detailed clause-by-clause interpretation of OSHA, EPA, DOT, PHMSA, or other regulations. The regulatory environment is complex and overlapping for some industry segments. Many industries are clearly covered by OSHA 1910.119 Process Safety Management, which makes a few specific mentions of alarms.

The important thing is that regulatory agencies have "general duty" clauses and interpretations. As one example, consider OSHA 1910.119 (d)(3) (ii) which states, "The employer shall document that equipment complies with recognized and generally accepted good engineering practices." This is actually a regulatory acronym, RAGAGEP.

Codes, standards, and practices are usually considered "recognized and generally accepted good engineering practices." In the OSHA interpretation letter to ISA, a National Consensus Standard, such as ISA-18.2, is a RAGAGEP. OSHA recognizes ANSI/ISA S84.01-1996 as an example.2 There exists a "Memorandum of Understanding" between OSHA and ANSI regarding these matters.[3]

There is little question ISA-18.2 is an example of RAGAGEP, and companies should expect the regulatory agencies to take notice. 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 has 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 used for enforcement reasons.

The U.S. Chemical Safety Board (www.csb.gov) will also be using ISA-18.2 as a resource in its investigations. Other regulatory agencies are also becoming aware of ISA-18.2. The American Petroleum Institute (API) will soon release API RP-1167, Alarm Management Recommended Practices for Pipeline Systems. This API document is in full alignment with ISA-18.2, and the Pipeline and Hazardous Materials Safety Administration (PHMSA) generally adopts API recommended practices in their regulatory language.

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 with codes, 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."

2. See http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=INTERPRETATIONS&p_id=25164
3. See http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=MOU&p_id=323

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

An immense amount of work was done in 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 response."*

6. Alarm State Transitions

ISA-18.2 includes a moderately complex diagram depicting the alarm states and sub-states of "Normal", "Unacknowledged", "Acknowledged", "Returned-to-Normal", and "Latched". Of particular interest are the states of "Shelved", "Suppressed by Design", and "Out of Service". These have specific meanings:

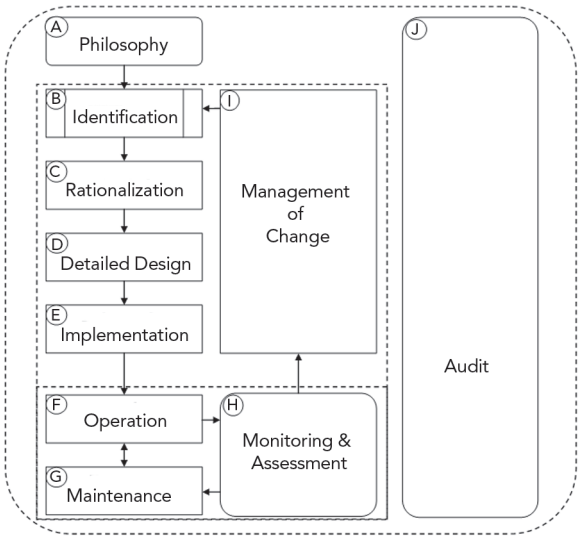

Figure 1: The Alarm Management Life Cycle

"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 due to 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 life cycle. 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 are used to 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 the detection of such undesirable situations is part of the Monitoring life cycle stage.

7. The Alarm Management Life Cycle

ISA-18.2 is written with a life cycle structure comprised of ten stages (see Figure 1). They are:

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 set forth in the alarm philosophy, including the tasks of prioritization, classification, settings determination, and documentation.

Detailed Design: The process of designing the aspects of the alarm so that it meets 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 due to either test or repair activities. (Do not equate this life cycle 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. Life Cycle Stages vs. Activities

Do not confuse a life cycle stage with an activity. Life cycle 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 life cycle 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: "Ah 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 as to whether it was originally specified by some particular process like a 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 a proper thing 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[4]: 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 3. That seems reasonable, but let's just check the online master alarm database for the reasons that resulted in that priority assignment. Hmmm, they look pretty good. If they did not, I could not change them myself. I need the Prioritization team 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 life cycle stages were briefly visited in accomplishing this one example task. In understanding and applying ISA-18.2, do not get overwrought about trying to figure out which life cycle stage you are in at any point in time. It is a requirements structure, not a work process sequential checklist.

In 2006, PAS published T*he 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 life cycle methodology;

4. Documentation is a part of the Rationalization stage of the life cycle

there is only some different nomenclature and task arrangement.

8. The Alarm Philosophy Life Cycle Stage

ISA-18.2 recognizes that an alarm philosophy document is a key requirement for effective alarm management. A table lists topics which are noted as either 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, training, etc.

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 a variety of 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. There are no specific class requirements and no minimum number of class definitions specified. PAS recommends the "keep it simple" approach and have 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" or HMAs was chosen as the term. The intent is to identify the alarms that must have a considerably high level of administrative requirements.

Now, there is no requirement to have or use this classification. However, if you do, if you state "this classification in my philosophy is per the ISA-18.2 usage of Highly Managed", then you must document and handle a multitude of special administrative requirements in a precise way according to the standard.

The various mandatory requirements for HMAs are spread over several sections throughout ISA-18.2. These include:

- 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

PAS' advice is to specifically avoid the usage of this alarm classification. You might choose to have your own *similar* classification, and then choose only the administrative requirements you deem necessary for those alarms. These will probably be only a subset of the ISA-18.2 listing for HMAs.

9. The Alarm System Requirements Specification (ASRS)

This non-mandatory section basically says that if you are buying 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 Life Cycle 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 for use of one of those types or the creation of a specific alarm via custom logic or calculation may be driven from a variety of process-related sources. These are the usual list of studies such as a Process Hazard Analysis (PHA), Layer of Protection Analysis (LOPA), Failure Mode and Effects Analysis (FMEA), etc.

11. The Alarm Rationalization Life Cycle Stage

This life cycle 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, setpoints, etc. In ISA-18.2, the word is used to indicate a collection of activities that may be done in a variety of 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, consequences, etc.
- Determining the alarm's classification

Note all of the activities listed above include both the cases of 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. Some examples of such methods are planned for one of the follow-up ISA technical reports.

12. The Basic Alarm Design Life Cycle 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. Since there is a current ISA standard in development specifically about HMIs (ISA-101), this section is intentionally limited.

Some items discussed (with little detail), include:

- Depiction of alarm states, priorities, and types
- Alarm silencing and acknowledgement
- 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

Many functionality items are 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. It is noted at the start of the section that some described features are not possible in some control systems. You can still be in compliance with the standard if you have such a system.

I would estimate that the ISA-101 standard on

HMI is several years from issuance. It actually might turn out to be just a technical report than a standard; this is uncertain. In the meantime, if you want more detailed information on creating proper and effective operator graphics, we recommend our latest book *The High Performance HMI Handbook*, as well as the *ASM Consortium Guidelines for Effective Operator Display Design*.

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 modification
- State-based alarming
- Model-based alarming
- Non-control room considerations (such as remote alarm notification)
- 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 Life Cycle 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 Life Cycle 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 Life Cycle 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 life cycle, 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 in regard to equipment replacement

18. The Monitoring and Assessment Life Cycle Stage

This is the stage in which alarm system performance is measured and reported. The intent is to verify that the other life cycle stages are successful in creating an alarm system that is effective.

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. The numbers allow for possible modifications, and are as follows:

"The target metrics in the following sections are approximate and depend upon many factors (e.g. 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."

The analyses described are:

- Average annunciated alarm rate per operating position (per day, 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)
- Alarm attributes priority distribution (alarm configuration)
- Unauthorized alarm suppression
- Alarm attribute monitoring (for unauthorized change)

In deciding the particular measures and performance numbers, the committee did considerable research to achieve consensus. Several analyses with problematic concerns were intentionally left out. Recommendations for the reporting of alarm system analyses are provided.

19. The Management of Change Life Cycle 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 Life Cycle 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. Summary

ISA-18.2 is an important standard and will undoubtedly result in a significant safety enhancement for the process industries. It validates and embodies practices that industry experts and leading manufacturing companies have advocated for many years. The publication of ISA-18.2 has significant regulatory consequences, and companies are advised to become familiar with its contents.

About the Author

Bill Hollifield is the PAS Principal Alarm Management and HMI Consultant. He is a voting member of the ISA SP-18 Alarm Management committee and the American Petroleum Institute's committee developing *API-1167 Recommended Practices for Alarm Management of Pipeline Systems*. Bill is also the coauthor of *The Alarm Management Handbook*, *The High-Performance HMI Handbook*, and the *Electric*

Power Research Institute's Alarm Management and Annunicator Application Guidelines. Bill has international, multi-company experience in all aspects of Alarm Management along with many years of chemical industry experience with focus in project management, chemical production, and control systems.

Bill holds a Bachelor's Degree in Mechanical Engineering from Louisiana Tech University and an MBA from the University of Houston. He's a pilot, and builds furniture (and the occasional log home in the Ozarks) as a hobby.

About PAS

PAS (www.pas.com) improves the automation and operational effectiveness of power and process plants worldwide by aggregating, contextualizing, and simplifying relevant information and making it universally accessible and useful. We provide software and services that ensure safe running operations, maximize situation awareness, and reduce plant vulnerabilities. Our comprehensive portfolio includes solutions for Alarm Management, Automation Genome Mapping, Control Loop Performance Optimization, and High-Performance Human-Machine Interfaces. PAS solutions are installed in over 1,000 industrial plants worldwide.

Contact PAS:
16055 Space Center Blvd., Ste. 600
Houston, TX 77062
+1.281.286.6565
info@pas.com