OCTAVE

WHITE PAPER

# A well-kept secret: The ISA-18.2 technical reports on alarm management

# Introduction

Since the ISA-18.2 Alarm Management Standard was originally issued in 2009, a series of associated International Society of Automation (ISA) technical reports (TRs) have been created. The TRs expand on the content of the standard, providing informative content with examples.

In this white paper, we discuss the differences between standards and technical reports and the content of each TR. We then compare the content in *The Alarm Management Handbook, Second Edition*.

The author of this white paper participated in the development and content generation of all the ISA-18.2 TRs.

# Standards vs. technical reports: What's the difference?

"Standard" is a special word. A standard is an authoritative document developed in accordance with a strict American National Standards Institute (ANSI) methodology, embodying such principles as the balance of interests and consensus and incorporating a stringent review and documentation process. Standards are developed by organizations that follow such a work process, such as ISA and the American Society of Mechanical Engineers (ASME).

Standards attain a special status called RAGAGEP (recognized and generally accepted good engineering practice). Standards can and will be used by government regulatory agencies as the basis for fines and enforcement actions, just as if they were actual regulations. Many examples of this exist. Occupational Safety and Health Administration (OSHA) includes it in its presentations, and government agencies such as the Food and Drug Administration (FDA) mention it on their websites.

For those interested, Octave has a separate paper on octave.com covering this in more detail, "Understanding and Applying the ISA-18.2 Alarm Management Standard."

## Standards do not contain:

- Detailed examples, alternative methods or work processes, and which are preferred and under what circumstances
- "Optimum" practices or "good ideas you should try" or "general good advice"
- Lists of things to worry about
- Educational material, lecture or advocacy
- Details of other applicable standards. Those might be mentioned or placed in a references section
- Reminders or education about applicable regulatory requirements. There are no statements like "You should also become familiar with OSHA regulation ABCDEF123." You are expected to know the regulatory requirements of your industry

## What vs. how

The content of a standard is significantly and intentionally constrained. It covers the minimum acceptable requirements, not the optimum. Mandatory requirements (indicated by "shall") are clear and actionable. However, specific methods to accomplish those requirements are intentionally not provided. Recommendations (indicated by "should") are also offered but have no prescribed methods for accomplishment.

"Informative" content in a standard is kept to a minimum and is specifically identified as such. Information such as the history or nature of a problem is not provided, and the basics of relevant technology are not provided. The reader is expected to fully understand the underlying technology the standard addresses. You do not learn about a technology from reading a standard.

# ISA Technical reports

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 (TR). By design, nothing in a TR is mandatory.

TRs contain:

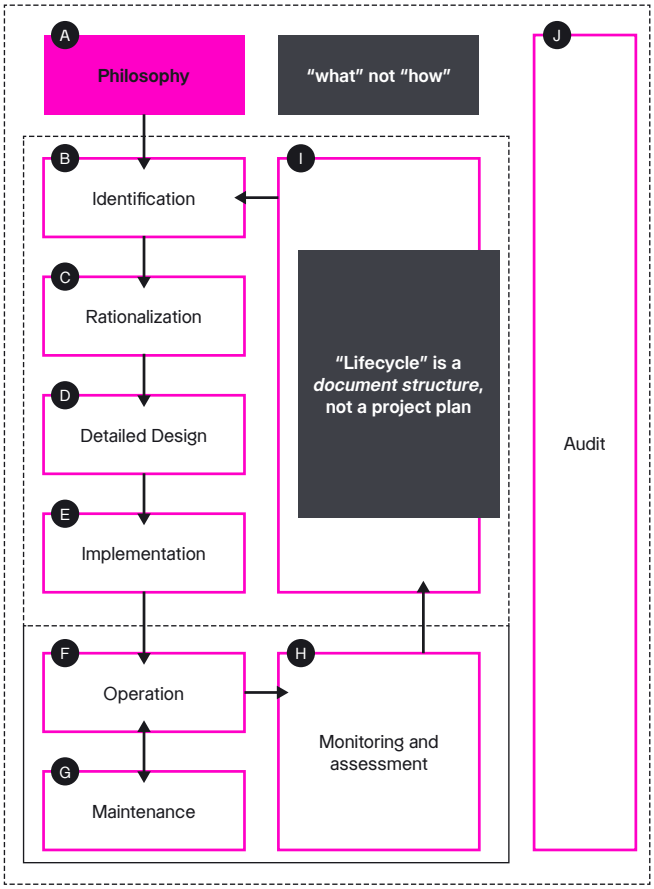
- Information on how to apply a standard
- Examples, alternatives and "how to" information, clearly marked as such. Those must also be proven in practice and recognized and generally accepted. Examples are vendor and product-neutral.
- Proven methods based on real-world experience
- Work processes with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

## Lifecycle

Most standards provide a framework of lifecycle steps and activities, usually reflecting a greenfield project sequential structure. However, lifecycle is a structure of requirements and documentation, not a project plan. Accomplishing steps in lifecycle order may be suboptimum for improving an existing system.

This is certainly the case for alarm system improvement, when compared to Octave's seven-step process, as detailed in *The Alarm Management Handbook*. The ISA-18.2 TRs are generally written to address each part of the lifecycle.

### ISA 18.2 and IEC 62682 Lifecycle




## Seven steps

The "what" and the "how." A concise approach to optimizing alarm systems.

**Step 1:** Develop, adopt and maintain an alarm philosophy

**Step 2:** Collect data and benchmark your systems

**Step 3:** Perform "bad actor" alarm resolution

**Step 4:** Perform alarm documentation and rationalization

**Step 5:** Implement alarm audit and enforcement technology

**Step 6:** Implement real time alarm management

**Step 7:** Control and maintain your improved system

**Figure 1:** ISA 18.2 Lifecycle and the seven-step process
**Sources:** The ISA-18.2 Alarm Management Standard and *The Alarm Management Handbook*

# Accessing ISA technical reports

ISA members can view most standards and technical reports online for free at www.isa.org. To download the report, however, viewers must purchase the document. The annual price of ISA membership is about the same as buying one document.

Here is a list of the current TRs. The process of creating a TR is a slow one. These are created by committees in the spare time of busy volunteers, so they may take considerable time to publish.

| Technical Report | Status |
|---|---|
| ISA 18.2 TR-1: Alarm Philosophy Document | 2018 |
| ISA 18.2 TR-2: Alarm Identification and Rationalization | 2016 |
| ISA 18.2 TR-3: Basic Alarm Design | 2015 |
| ISA 18.2 TR-4: Enhanced and Advanced Alarm Methods | 2012 |
| ISA 18.2 TR-5: Alarm System Monitoring, Assessment and Auditing | 2012 |
| ISA 18.2 TR-6: Alarm Systems for Batch and Discrete Processes | 2012 |
| ISA 18.2 TR-7: Alarm Management When Utilizing Packaged Systems | 2017 |
| ISA 18.2 TR-8: Alert Systems – Guidelines for Non-Alarm Notifications | 2023 |

**Figure 2:** List of ISA-18.2 Technical Reports

# TR1: Alarm philosophy document

Most alarm systems perform poorly because they were initially configured without the guidance of an alarm philosophy document incorporating proper principles. ISA-18.2 mandates the creation of such a document and provides some basic information about its necessary and desired content. All ISA TRs contain an initial few sections, typically called scope, introduction, references and definitions. The definitions are repeated from ISA-18.2 for the convenience of the reader. In this paper, we will refer to this content collectively as the "boilerplate," being content (such as the legal disclaimers) that the reader generally skips over. Each TR's boilerplate typically consists of 15-17 pages.

After the boilerplate, TR1 has the following sections that total about 37 pages:

1. General
2. Identification
3. Rationalization
4. Detailed design
5. Implementation, operations and maintenance
6. Management of change
7. Monitoring and reporting
8. Audit
9. References

**Annex A:** Control system-specific capabilities and limitations

**Annex B:** Example: A comprehensive alarm philosophy table of contents

TR1 is limited to discussing ISA-18.2's clause 6 on alarm philosophy, which has only seven pages. It covers "what should be in the alarm philosophy document" for each alarm-related topic. The details of most of those topics are often in different ISA technical reports. TR1 is comparatively short.

ISA-18.2 contains "table 3 - required and recommended alarm philosophy content," shown below, with content noted as required or recommended. Notes are added to the right.

| Alarm philosophy contents | Required / recommended | Sub-clause |
|---|---|---|
| Purpose of alarm system | Required | 6.2.2 |
| Definitions | Required | 6.2.3 |
| References | Recommended | 6.2.4 |
| Roles and responsibilities for alarm management | Required | 6.2.5 |
| Alarm design principles | Required | 6.2.6 |
| Alarm setpoint determination | Recommended | 6.2.7 |
| Prioritization method | Required | 6.2.8 |
| Alarm class definition | Required | 6.2.9 |
| Highly managed alarms (or site equivalent) | Recommended | 6.2.10 |
| Rationalization | Required | 6.2.11 |
| Alarm documentation | Required | 6.2.12 |
| Alarm design guidance | Required | 6.2.13 |
| Specific alarm design considerations | Recommended | 6.2.14 |
| HMI design principles | Required | 6.2.15 |
| Approved enhanced and advanced alarming techniques | Recommended | 6.2.16 |
| Implementation guidance | Required | 6.2.17 |
| Alarm response procedures | Required | 6.2.18 |
| Training | Required | 6.2.19 |
| Alarm shelving | Recommended | 6.2.20 |
| Alarm system maintenance | Required | 6.2.21 |
| Testing of alarms | Required | 6.2.22 |
| Alarm system performance monitoring | Required | 6.2.23 |
| Alarm history preservation | Recommended | 6.2.24 |
| Management of change | Required | 6.2.25 |
| Alarm Management Audit | Required | 6.2.26 |
| Related site procedures | Recommended | 6.2.27 |

**The alarm philosophy must address:**

How to select items to be alarms

Highly managed are not required. Do not use that class

Criteria for rationalization and alarm info to be captured and maintained

Alarm types, deadband/delay-time use, alarm messages and more

Not required but important and can save you money

Specify symbols, colors, sounds and functions of ACK and SIL

Commissioning, checkout, training, procedure details and access

Handling out-of-service alarms, record keeping, testing documentation

Ongoing alarm system analysis and annual performance report

**Figure 3:** Required and recommended alarm philosophy content
**Source:** The ISA-18.2 Alarm Management Standard

Short paragraphs about each item follow in the 18.2 document, and TR1 goes into more detail about each one with examples. TR1 contents include:

### TR1 Section 4: Introduction (nine pages).

This covers a brief introduction to the purpose and use of a philosophy document, general information about alarms and alarm states and similar basic concepts.

### Section 5: Alarm identification (one page).

**Note:** TR2 addresses this topic more fully. This section contains a list of sources for identifying potential conditions that should be alarmed.

### Section 6: Alarm rationalization and documentation (five pages).

**Note:** TR2 addresses these topics more fully. This section contains:

- Recommended team approach and makeup
- Example matrix for determining alarm priority
- Example methods for determining alarm setpoints
- Recommendations for items to be included in alarm documentation
- The creation and maintenance of the mandatory master alarm database (MADB)
- Examples of determining alarm classification, including the highly managed classification, which should not be used

# An aside: What is the problem with highly managed alarms?

ISA-18.2 introduces the concept of alarm classification and the particular class of highly managed alarms. This topic causes more misunderstandings and questions than any other for ISA-18.2. We address it in the *"Understanding and Applying the ISA-18.2 Alarm Management Standard,"* but it bears repeating (with some additional information) here. Alarm classification tracks administrative requirements for groups of alarms, such as special procedures, training and testing.

- Alarm classes are defined and used to keep track of administrative requirements. Think of an alarm class as a bucket. Administrative requirements that apply to alarms within the bucket are written on it.
- Alarms can be assigned to more than one classification
- Classification is not "alarm priority" or "alarm type" or "alarm purpose"
- No specific classes are required in 18.2, and no minimum number of class definitions are required. Having only a single class is acceptable and is used by some with simple processes

We recommend keeping it simple when determining your alarm classifications. We often find that four classes are adequate. You do not want to have many separate alarm classifications overlapping regarding their requirements. Designating your classes simply based on their administrative requirement is much simpler.

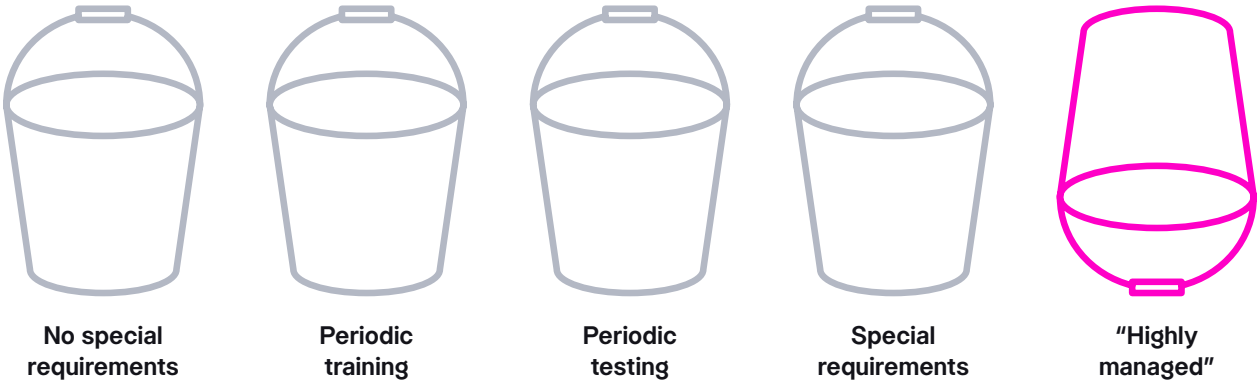



**Figure 4:** Alarm classification buckets made simple and straightforward

# Highly managed alarms

ISA-18.2 specifically defines only one classification of alarms, highly managed alarms. There is no requirement to name any alarms to this class. If you designate any alarms as highly managed, you must perform 38 explicitly identified ISA 18.2 administrative requirements listed below.

As you investigate the list, you may determine that some requirements are reasonable for some of your most important alarms, and the rest may not apply. But, if you call your classification highly managed, you must perform all 38 requirements to comply with ISA-18.2. This is likely a lot of pointless and wasted effort.

For practical compliance, if you have a few very important alarms for which you have several administrative requirements, then make your classification for them, listing only the items you require. And don't call that classification "highly managed." There is no benefit from using this specific ISA-18.2 classification.

| | ISA-18.2-2009 | ISA-18.2-2016 | IEC-62682-2014 |
|---|---|---|---|
| HMA requirements must be documented in the alarm philosophy | 6.2.7.1 (1 item) | 6.2.10 (1 item) | 6.2.9 (2 items) |
| Access controls for mandatory requirements for highly managed alarms (HMAs) shelving of HMAs | 11.7.1 (1 item) | | |
| Access controls to place HMAs out-of-service | 11.8.1 (1 item) | | |
| Initial operator response training and documentation requirements | 13.3.1 (1 item) | 13.3.3 (4 items) | 13.3.4 (4 items) |
| Initial operator response training and documentation requirements | 13.3.1.1, 13.3.1.2 (8 items) | | |
| Philosophy document must identify HMA testing requirements | 13.4.1 (1 item) | 13.4.2 (1 item) | 13.4.2 (1 item) |
| Nine items must be documented in the initial testing | 13.4.1 (9 items) | 13.4.2 (9 items) | 13.4.2 (9 items) |
| Requirements and documentation for shelving HMAs | 14.3.2 (2 items) | 14.3.2 (4 items) | 14.3.2 (4 items) |
| HMA refresher training is required with items of documentation | 14.4.1 (5 items) | 14.4.2 (6 items) | 14.4.2 (6 items) |
| Mandatory periodic training is required, with items that must be covered | 14.4.2 (4 items) | 14.4.3 (3 items) | 14.4.3 (3 items) |
| Mandatory periodic testing is required, with a requirement for repair or special procedures and documentation | 15.2.1 15.2.2 (8 items) | 15.2.3 15.2.4 15.2.5 (7 items) | 15.2.3 15.2.4 (4 items) |
| Mandatory interim alarms or procedures for out-of-service alarms | 15.3.2 (1 item) | 15.3.3 (1 item) | 15.3.3 (2 items) |
| Mandatory refresher training is required, with items of documentation | 15.7.1 (5 items) | 15.6.2 (3 items) | 15.6.2 (3 items) |
| Audit requirement for HMAs | 18.2.1 (1 item) | | |
| **Total Items** | **46 items** | **38 items** | **38 items** |

**Figure 5:** Mandatory requirements for highly managed alarms (HMAs)

# HMA requirements in standards documents

**Section 7:** Alarm design (13 pages). Note: TR3 addresses these topics more. This section contains information about various alarm features and capabilities. A short special alarm design considerations section focuses on pre-determining alarm approaches for many everyday situations. Hexagon recommends that this be a substantial part of an AP document because it can save time and money in alarm rationalization.

**Section 8:** Implementation, operation and maintenance (four pages). This section includes information on training, testing, documentation and procedures.

**Section 9:** Management of change (one page). This section provides examples of what aspects of an alarm system should be under a management of change (MOC) regimen and approaches to alarm system MOC.

**Section 10:** Alarm system performance monitoring (two pages). Note: TR5 addresses these topics more. This section includes the metrics table repeated from ISA-18.2 and some discussion of alarm periodic reporting, distribution and alarm history preservation.

**Section 11:** Alarm audit (one page). Note: TR5 addresses this topic more. This section contains the nature and purpose of a periodic (typically annual) audit of alarm system management practices.

**Section 12:** References non-normative (one page). References are external documents that were used in creating the technical report. They are not "reading lists." The section provides a short list that includes books from Octave, *The Alarm Management Handbook* and The High Performance HMI Handbook.

**Annex A:** Control system specific capabilities and limitations (one page). This short section discusses the differences in alarm system capabilities of contemporary control systems.

**Annex B:** Example comprehensive alarm philosophy table (three pages). This section is pulled directly from *The Alarm Management Handbook, Second Edition*.

## Comparison of TR1 to *The Alarm Management Handbook*

*The Alarm Management Handbook* contains significantly more information about each topic in each section than ISA-18.2 or TR1. Significant parts are pulled from the handbook, including the example table of contents of a comprehensive alarm philosophy document. The handbook puts forth a method by which you can create a customized and comprehensive philosophy document that matches your internal work practices, complies with ISA-18.2, and contains best practices proven in the industry.

# TR2: Alarm identification and rationalization

TR2 has 17 pages of boilerplate and 22 pages of content. The content sections are:

- Project scoping
- Identification
- Rationalization (approaches, team methodologies, resources, roles and processes)
- Prioritization (typical methods and examples)
- Alarm classification (typical approaches)
- Master alarm database and alarm documentation (software, contents, accessibility and uses)
- Altering the alarm system to reflect the master alarm database (approaches to MOC issues and training)
- Bibliography
- Appendix A – potential pitfalls to success (a list of things to worry about)

Identification is the task of finding conditions that might need alarms. TR2 discusses these methods and sources:

- Existing (already configured) alarms
- Alarms the control system can generate as "standard" based on the type of measurement
- Alarms from process safety studies, such as:
    - PHA: Process hazards analysis
    - HAZOP: Hazards and operability study LOPA: layers of protection analysis
    - FMEA: Failure modes and effects analysis
- Environmental permit limits
- Product quality limits
- Incidents
- Operating procedures
- Equipment manufacturer
- Alarm philosophy (defaults or pre-defined alarms)

In rationalization, potential alarms from the identification step are compared to the criteria in the alarm philosophy for suitability. Several tasks are accomplished in rationalization and discussed in the TR. These include:

- Alarm verification
- Prioritization (typical methods and examples)
- Alarm classification (typical approaches). Master alarm database and alarm documentation (software, contents, accessibility and uses)
- Altering the alarm system to reflect the master alarm database (approaches to MOC issues and training)

Approaches to accomplishing these tasks, such as team methodologies, resources, roles and processes, are briefly discussed. A substantial amount of the content comes from *The Alarm Management Handbook*.

## Comparison of TR2 to *The Alarm Management Handbook*

Rationalization is the most expensive and resource-consuming task you will do in alarm management. The TR covers it in about 15 pages. In contrast, the handbook has over twice as many pages of detailed content dedicated to this subject, including tips, efficiency advice and practices proven through hundreds of successful projects.

# TR3: Basic alarm design

TR3 has 20 pages of boilerplate and 29 pages of content. Much of the content was obtained from the handbook. The contents cover:

- Basic alarm design considerations
- Alarm sources
- Usage of alarm states
- Alarm types (absolute, deviation, rate-of-change, discrepancy, discrete, diagnostic, operator-adjustable, first-out, common and more)
- Alarm attributes (alarm setpoint, range, deadband, on/off delay, priority and message)
- Programmatic changes to alarm attributes
- Alarm design for specific applications (safety system, trips, call-out and packaged systems)
- Review alarm configuration (for management-of-change)
- Operator span of control/routing of alarms
- Alarm performance metrics (relevant to alarm design or configuration, see TR5)
- References
- Bibliography

TR3 includes a basic discussion of the following:

- Alarm states (normal, unacknowledged, acknowledged, return-to-normal, shelved, designed suppression or out of service)
- Use of alarm state in interlocks
- Re-alarming, latching and shelving
- Basic discussion of alarm types and issues with their use (absolute, deviation, rate-of-change, discrepancy, discrete, first-out, common and more)
- Diagnostic alarms on sensors
- Alarms from fieldbus/profibus architectures
- Guidance for design of operator-adjustable alarms
- Operating range and alarms
- Determining alarm setpoints, deadbands and delay times
- Chattering and fleeting alarm analysis and solution
- Effective alarm messages
- Specific alarm design considerations (safety system, trips, call-out, packaged systems – a short list)

### Comparison of TR3 to *The Alarm Management Handbook*

The handbook has significantly more content on these topics than does TR3. For example, it has an entire chapter on detecting and solving nuisance alarm behaviors. It contains over a dozen specific pre-defined alarm designs, that save significant time during rationalization.

## TR4: Enhanced and advanced alarm methods

TR4 is based on a short, information-only section in ISA-18.2 called "detailed design: enhanced and advanced alarm methods." TR4 has 17 pages of boilerplate and 37 pages of content. TR4 has the following sections:

- Considerations in the application of enhanced and advanced alarming methods
- Information linking
- State-based alarming
- Dynamic cause analysis and guidance
- Alarm routing and escalation

- Use of alerts
- Advanced alarming relative to batch and discrete operations
- Work process and preservation of alarm integrity
- References and bibliography

TR4 provides more informative content on these topics:

- State-based alarming: control systems provide for single alarm settings. If processes operate in different states, which is often the case, the alarm settings should be different.
- A rationalized alarm system may still experience alarm flooding, and flood solutions are discussed
- Operators need easy access to the alarm documentation created in the rationalization step
- The operator may not be the only role that needs to receive an alarm
- The use of separate operator alert systems

In ISA-18.2, "enhanced and advanced" alarm methods apply to these situations. It is noted that their implementation may involve additional cost and engineering time.

### Comparison of TR4 to *The Alarm Management Handbook*

All the TR4 content is contained in the handbook in more detail. Octave has been supplying advanced alarm technologies, including state-based alarming, for years prior to the creation of ISA-18.2.

## TR5: Alarm system monitoring, assessment and auditing

TR5 has 20 pages of boilerplate and 45 pages of content. The content sections are:

- Alarm systems and human factors (operator response, rates, averages, differences and operating staff)
- Periodic alarm system performance reporting (performance and diagnostic reports)
- Alarm system analyses for monitoring and assessment (ISA-18.2 key alarm metrics, rates per time, floods, frequent, chattering, fleeting, types, stale, priority, correlation, acknowledgment, MOC and more)
- Alarm system auditing
- Alarm data (types, configuration and occurrence records)
- Methodologies for obtaining alarm data
- References

TR5 contains the ISA-18.2 "weasel words." The target metrics are approximate and depend upon many factors (i.e., 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. TR5 discusses those concepts and then discusses all the ISA-18.2 metrics.

## Alarm performance metrics based on 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 day per operating position | ~ 150 alarms per day | ~ 300 alarms per day |
| Annunciated alarms per hour per operating position | ~ 6 (average) | ~ 12 (average) |
| Annunciated alarms per 10 minutes per operating position | ~ 1 (average) | ~ 2 (average) |

| Metric | Target Value |
|---|---|
| Percentage of hours containing more than 30 alarms | ~< 1% |
| Percentage of 10-minute periods containing more than 10 alarms | ~1<% |
| Maximum number of alarms in a 10-minute period | ≤ 10 |
| Percentage of time the alarm system is in a flood condition | ~< 1% |
| 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, with 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-purposes priorities excluded from the calculation |
| Unauthorized alarm suppression | Zero alarms suppressed outside of controlled or approved methodologies |
| Unauthorized alarm attribute changes | Zero alarm attribute changes outside of approved methodologies or MOC |

**Figure 6:** Alarm performance metric summary from ISA-18.2
**Source:** The ISA-18.2 Alarm Management Standard Technical Report 5 (2009)

TR5 then continues and discusses several useful measurements that are not on the ISA-18.2 list, along with these concepts:

- Why averages can be misleading
- Effect of alarm response differences in rates and averages
- Examples of effective alarm performance visualization
- Alarm priority: occurrences vs. configuration
- Remedial actions to take based on specific measurements
- Operating staffing models/assignments vs. alarm rates
- Customized reports for different audiences
- Detecting alarm changes relative to MOC
- Analysis of operator action records relevant to alarms
- Examples of alarm record contents and structure

There are many figures. All this information is in *The Alarm Management Handbook*.

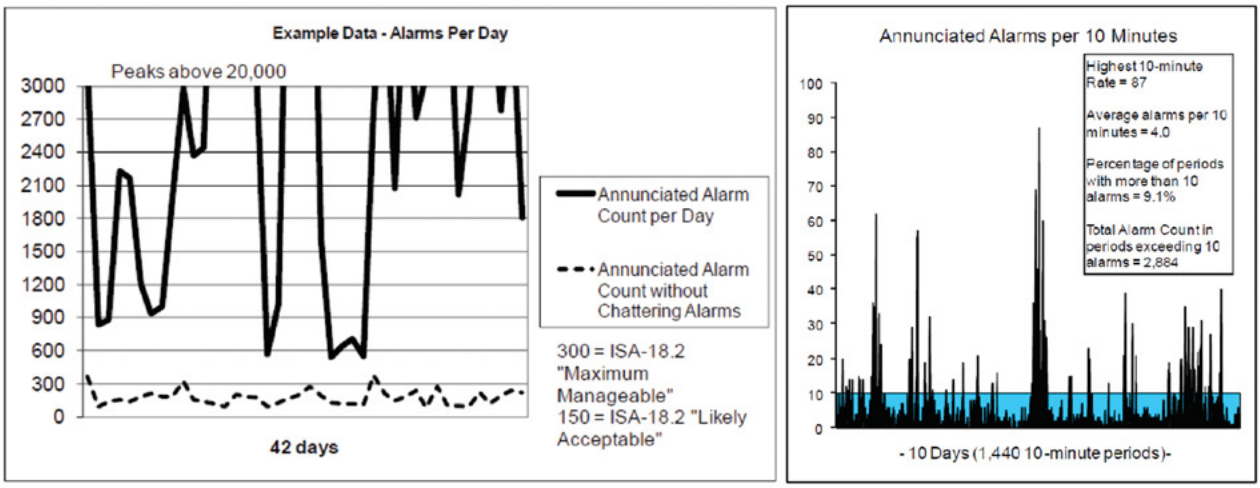



**Figure 7:** Example Figures in TR5
**Source:** The ISA-18.2 Alarm Management Standard Technical Report 5 (2009)

# TR6: Alarm systems for batch and discrete processes

TR6 is different than the other TRs. It covers all of ISA-18.2, not just a specific lifecycle step. TR6 has 18 pages of boilerplate and 51 pages of content. The content sections are:

- Continuous, batch and discrete processes
- Alarm system models
- Philosophy
- Alarm system requirements specification
- Identification
- Rationalization
- Basic alarm design
- HMI design
- Enhanced/advanced alarming
- Implementation
- Operations
- Maintenance
- Monitoring and assessment
- Management of change (MOC)
- Audit
- References and bibliography

The initial response of some of the batch and discrete manufacturing community to ISA-18.2 was that it seemed to have a very continuous-process flavor, and the relevance of it to their processes was questioned. The purpose of TR6 was to show the community how each part of ISA-18.2 applies to those processes. Some of the special considerations for batch and discrete processes covered in TR6 are:

- Alarm analysis: records need to relate to specific batches
- Alteration of alarms for various batch phases (the potential for more use of state-based alarming in batch processes)
- Regulatory issues for retention of alarm records
- Emphasis on alarms relating to product quality
- Continuous alarm setpoint variation during ramping operations
- Alarms for product transitions
- Various alarm-related regulatory issues, such as alarm testing and system validation and qualification (i.e., in pharmaceuticals)
- Alarms and the connection to the ISA-88 Batch model terminology

TR6 is recommended reading for those with batch processes. It has content that is not in *The Alarm Management Handbook*.

# TR7: Alarm management when utilizing packaged systems

A packaged system is a self-contained combination of hardware and software with an alarm, human-machine interface (HMI) and control functionality for a specific process function. It is part of a facility provided by a single specialized vendor.

Like TR6, TR7 is also different than the other TRs. It covers all of the ISA-18.2 lifecycle, but as it applies to the incorporation into the process of a packaged system.

Typical examples of a packaged system include a skid-mounted refrigeration unit or a complex process analyzer. The purpose of TR7 is to provide more detail about the alarm-related issues when integrating complex packaged equipment into an overall alarm system. Each 18.2 life cycle step is discussed for issues associated with using packaged equipment.

TR7 has 18 pages of boilerplate and 48 pages of content. The content is:

- What is a packaged system?
- Advantages of packaged system alarm management
- Packaged system control panels
- Packaged system interfacing details
- Alarm philosophy
- Alarm system requirements specification
- Alarm identification
- Rationalization
- Basic alarm design for packaged systems
- Alarm routing
- HMI representation of alarms
- Implementation
- Operations
- Maintenance
- Monitoring and assessment
- Management of change
- Audit
- References and bibliography

Packaged systems (PSs) are implemented along a continuum of connectivity to the basic process control system (BPCS). Three levels of connectivity are characterized as standalone, semi-integrated and fully integrated.

The degree of integration significantly affects various aspects of alarm management. Additionally, processes utilizing many packaged systems may have some differences in the operator staffing and role models compared to a continuously manned control room. Roaming operators, for example, might be more common. The packaged system control panel (PSCP) is also a significant issue that must be addressed for alarm integration.

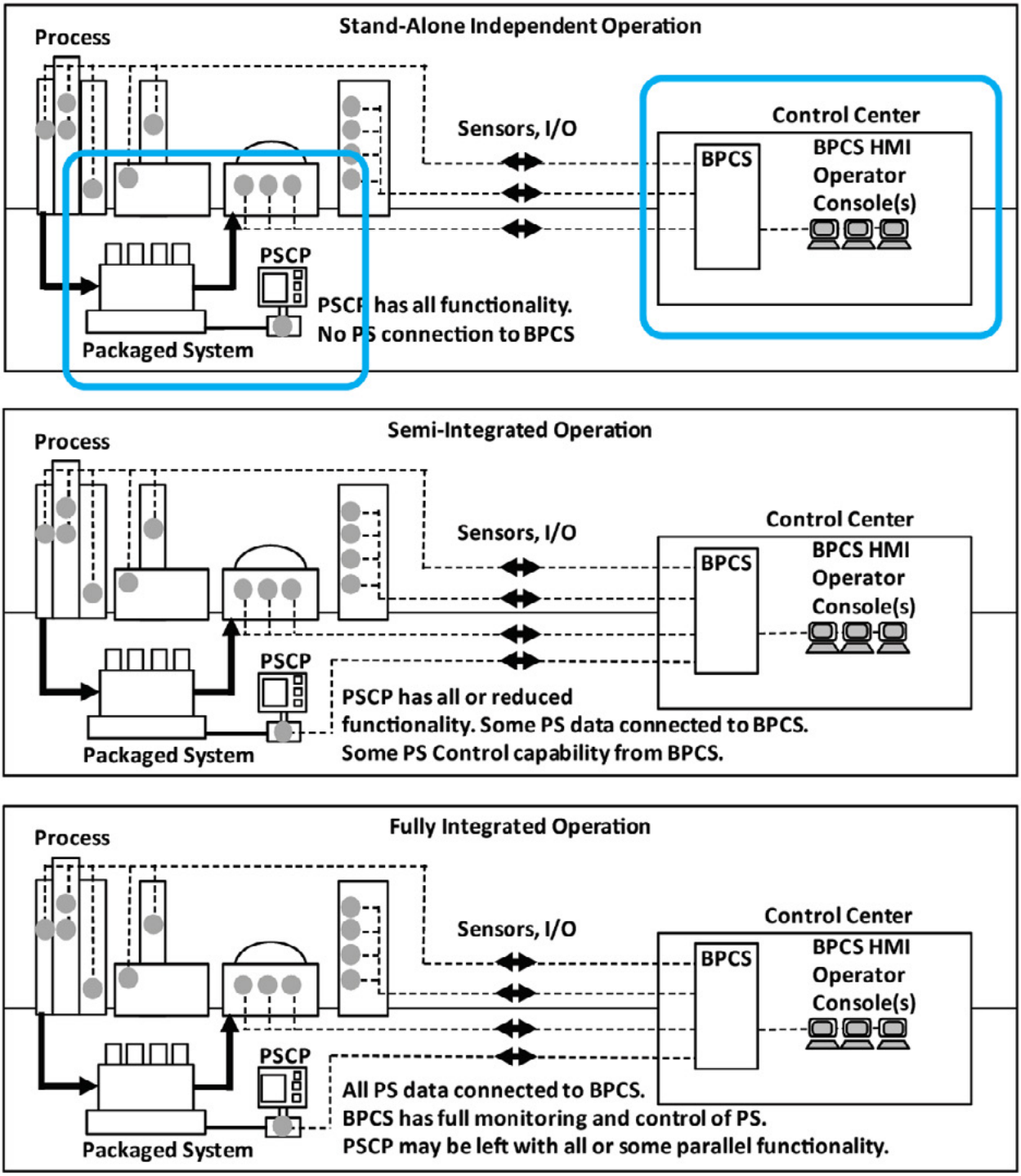



**Figure 8:** Packaged systems: Degree of integration with the BPCS
**Source:** The ISA-18.2 Alarm Management Standard Technical Report 7

| Packaged system control panel operational characteristics | Stand-alone independent operation | Semi-integrated operation | Fully integrated operation |
|---|---|---|---|
| Typical operator staffing model for PS monitoring | Dedicated roaming operator or an operator with both console and roaming duties | Dedicated roaming operator, or operator with both console and roaming duties, or console operator and roaming operator | Console operator present whenever the process is running directing duties of roaming operator(s) |
| Nature of the PS data connection to the BPCS | No connection | Hardwiring of individual sensors or serial, bus-type or network connection, based on the quantity of I/O | Usually, a bus-type or network connection based on the quantity of I/O |
| Location and nature of the annunciation of PS alarms | PSCP only | Alarming of significant problems via common or group alarms in the BPCS, detailed alarm or PS status available in the PSCP | Comprehensive and detailed alarming and indication of PS status in the BPCS. PSCP only used for specialized diagnosis of PS issues |
| Location, nature and responsibility for the Initial operator detection of PS alarms | At the PSCP, the roaming operator may involve significant time delay between annunciation and detection | At the BPCS by the console operator for some PS alarms (often grouped or common alarms). Obtaining details may require accessing the PSCP and some time delay | At the BPCS by the console operator, with no delay for a normally manned console |
| Diagnosis and response to PS alarms | Roaming operator at PSCP only | Some capabilities for diagnosis from readings available in the BPCS, details may require accessing the PSCP involving cooperation of console and roaming operator | Almost all diagnoses can be made by the console operator from information made available in the BPCS |
| Control of the PS | PSCP only | Some control functions are possible from the BPCS, others solely in the PSCP | Functionality for full control of the PS capable from the BPCS. |

**Figure 9:** Example: PSCP operational characteristics related to the degree of integration
**Source:** The ISA-18.2 Alarm Management Standard Technical Report 7

TR7 discusses:

- Examples of PSs
- Common problems with packaged system alarm capabilities
- Issues with HMI commonality
- Issues with alarm detection and acknowledgment
- Data communication methods, issues and robustness
- Accomplishing alarm generation and handling in the DCS instead of the PS
- Lack of PS alarm priorities
- ISA-18.2 alarm and HMI recommendations vs. typical PSCP capabilities and limitations

## Comparison of TR7 to *The Alarm Management Handbook*

TR7 is recommended reading for those with processes incorporating packaged systems. The handbook's section on alarms from external devices deals with the proper principles for incorporating alarms from separate, complex equipment. TR7 goes into more detail on those issues.

# Summary

The seven current ISA-18.2 technical reports on alarm management are useful resources. However, in *The Alarm Management Handbook, Second Edition*, all the topics in ISA 18.2 Technical Reports 1, 2, 3, 4, and 5 are covered in more detail and with much more real-world, practical and proven advice.

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.

# About the author

**Bill R. Hollifield**
Retired principal alarm management and HMI consultant

Bill is a retired principal consultant 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.