GUIDELINES FOR NON-ALARM NOTIFICATIONS

Title page, copyright, and preface by ISA

CONTENTS

GUIDELINES FOR NON-ALARM NOTIFICATIONS

FOREWORD

In 2009, ANSI/ISA-18.2-2009 Management of Alarm Systems for the Process Industries, commonly referred to as ISA-18.2, was issued, and later updated in 2016. The ISA18 committee established working groups to develop and maintain a series of technical reports with guidance on how to implement the practices outlined in ISA-18.2. The independent technical reports are described here.

- ISA-18.02.01 Alarm Philosophy [TR1], provides guidance on the alarm philosophy. TR1 is limited to the scope of clause 6 in ISA-18.2. The alarm philosophy provides guidance for successful management of the alarm system. It covers the definitions, principles, and activities by providing overall guidance on methods for alarm identification, rationalization, classification, prioritization, monitoring, management of change, and audit.
- ISA-18.02.02 Alarm Identification and Rationalization [TR2], provides guidance on alarm identification and rationalization. TR2 was limited to the scope of clauses 8 and 9 in ISA-18.2. Identification and rationalization covers the activities to determine the possible need for an alarm or a change to an alarm; systematically compare alarms to the alarm philosophy; and determine the alarm setpoint, consequence, operator action, priority, and class. Activities include, but are not limited to, identification, justification, prioritization, classification, and documentation.
- ISA-18.02.03 Basic Alarm Design [TR3], provides guidance on basic alarm design. TR3 focuses on the scope of clause 10 of ISA-18.2 and may include other clauses as needed (e.g., clause 14 on operations and clause 15 on maintenance). Basic alarm design covers the selection of alarm attributes (e.g., types, deadbands, and delay times) and may be specific to each control system.
- ISA-18.02.04 Enhanced and Advanced Alarm Methods [TR4], provides guidance on advanced and enhanced alarm methods. TR4 focuses on the scope of clause 12 of ISA-18.2. Enhanced alarm design covers guidance on additional logic, programming, or modeling used to modify alarm behavior. These methods may include: dynamic alarming, state-based alarming, adaptive alarms, logic-based alarming, predictive alarming, as well as most of the designed suppression methods.
- ISA-18.02.05 Alarm Monitoring, Assessment, and Audit [TR5], provides guidance on monitoring, assessment and audit of alarms. TR5 focuses on the scope of clauses 16 and 18 in ISA-18.2. Monitoring, assessment, and audit cover the continuous monitoring, periodic performance assessment, and recurring audit of the alarm system.
- ISA-18.02.06 Alarm Systems for Batch and Discrete Processes [TR6], provides guidance on the application of ANSI/ISA-18.02 alarm life cycle activities to batch and discrete processes, expanding on multiple clauses of ISA-18.2.
- ISA-TR18.2.07 Alarm Management When Utilizing Packaged Systems [TR7], provides guidance on how to integrate packaged systems into a BPCS-based centralized alarm system.

The guidance as presented in this document is general in nature and should be applied to each system as appropriate by personnel knowledgeable in the manufacturing process and control systems to which it is being applied. This guidance will evolve with experience and technology advancements.

INTRODUCTION

This technical report provides a system of nomenclature for notifications other than alarms, and guidance on managing notifications generated by automation systems. This TR goes beyond the scope of ISA18.2 to include notifications to non-operator recipients. Guidance is provided on common terminology and recommended practices for generating and using such notifications.

GUILDELINES FOR NON-ALARM NOTIFICATIONS

1 Scope

This technical report was written in support of the standard ANSI/ISA-18.2-2016, Management of Alarm Systems for the Process Industries. The standard concerns itself with alarms for the operator role.

Modern automation-related systems are capable of creating many other types of notifications and routing them to roles other than the operator. This technical report defines notifications, with sub-types of alert, prompt, and notice for non-operator roles. Operator alerts and operator prompts are defined and discussed, taking into account the differences of the operator role. Recommendations and guidance for effective notifications are provided.

The definitions and terminology in this TR are general enough to encompass all possible notifications from the automation system to any role, without limiting the methods and equipment involved.

This Technical Report has connectivity to some topics in several other ISA standards, in which notifications from the automation system are discussed, such as ISA standards 84, 101, and 106.

This TR's intended audience are the designers, implementers, and maintainers of systems that generate automation system notifications, as well as the recipients of those notifications.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

3.1 Introduction

All ANSI/ISA 18.2:2016 definitions apply, except for the definition of alert which is redefined in this TR.

A distinction is made between the operator role (as specified in ANSI/ISA 18.2:2016) and non-operator roles.

3.2 Definitions

3.2.1
alarm
audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a timely response

3.2.2
alert
urgent or important notification that may require timely response

Note 1 to entry: This definition replaces the definition of alert in ANSI/ISA 18.2-2016

3.2.3
event
record of a change of state or value related to process data

3.2.4
human machine interface
HMI
collection of hardware and software used by the operator and other users to monitor and interact with the control system and with the process via the control system

3.2.5
notice
notification that is informational, useful, or of interest to the recipient

3.2.6
notification
transmission of an event to a recipient

3.2.7
operator alert
audible and/or visible means of indicating to the operator an equipment or process condition for evaluation when time allows which could result in a response

3.2.8
operator prompt
notification to the operator related to process continuance that requires timely response

3.2.9
prompt
alert related to process continuance that requires timely response

Note 1 to entry: task, data input, authorization, approval, permission to proceed

3.2.10
recipient
intended receiver of a notification

3.2.11
response
act of addressing the content of a notification

3.2.12
role
position, purpose or function that a user has in a relationship to the user interface of an automation or alarm system

EXAMPLE 1 ISA 101 section 4.1.1. quotes a number of user-roles as follows:

Operations - users who monitor and perform control and operation of the plant or facility (this may include both operators in the main control room as well as the extended operations team which may include remote users and users of portable interface devices);

Maintenance - users who perform troubleshooting and/or maintenance of the process, instrumentation and final control elements and rotating equipment;

Engineering - users who perform modifications, additions or deletions to the HMI or control system;

Administrators - users who perform updates to the control system itself, or assign security to other users;

Management - users who monitor the operation of the plant or facility;

Analysts - users who monitor the system to improve plant performance;

Others - users who use or interact with system for other purposes, for example, quality management personnel.

Note 1 to entry: It should be noted that a single person can have different roles.

3.2.13
user interface
UI
the non-process automation related interface of a device used by a notification recipient

Note 1 to entry: The term User Interface is used in this report to differentiate between the operator's HMI and the more varied devices used by non-operator roles.

3.3 Symbols and abbreviated terms

BPCS: Basic Process Control System

DCS: Distributed Control System

HMI: Human Machine Interface

IEC: International Electrotechnical Committee \

MTTR: Mean Time To Repair

OPC: Open Platform Communications

PIMS: Process Information Management System

PLC: Programmable Logic Controller

SCADA: Supervisory Control And Data Acquisition

SIF: Safety Instrumented Function

SIS: Safety Instrumented System

SIL: Safety Integrity Level

SRS: Safety Requirements Specification

TR: Technical Report

UI: User Interface

4 The definitional structure

4.1 General

This section provides an explanation of the different terms used in this document, and of their hierarchy and relationships. The use of consistent terminology helps to define the needs and requirements of a notification system.

4.2 Definitions and decision trees

This TR adheres to the consistent use of the definitions in Section 3. For example, whenever the word "alert" is used, it means items that fully meet the definition. Readers may have other definitions or usages for these words, but those cannot be used in interpreting this TR.

This TR uses the (undefined) term “automation system” in the broad sense. An automation system includes BPCS, DCS, SCADA, PLC, process historians, work planning systems, portable sensors, or devices – anything that is associated with a process and can detect or create events related to that process.

Because the operator role has very specific duties related to the process, this TR uses the term “Operator Alert” to refer to alerts for operators, and “alert” to refer to all non-operator roles. There are two charts used to show relationships between the definitions and decision points.

This Figure 1 depicts the important terms used in this report and their relationships for recipient roles other than the operator. The Figure 2 is for the Operator Role.

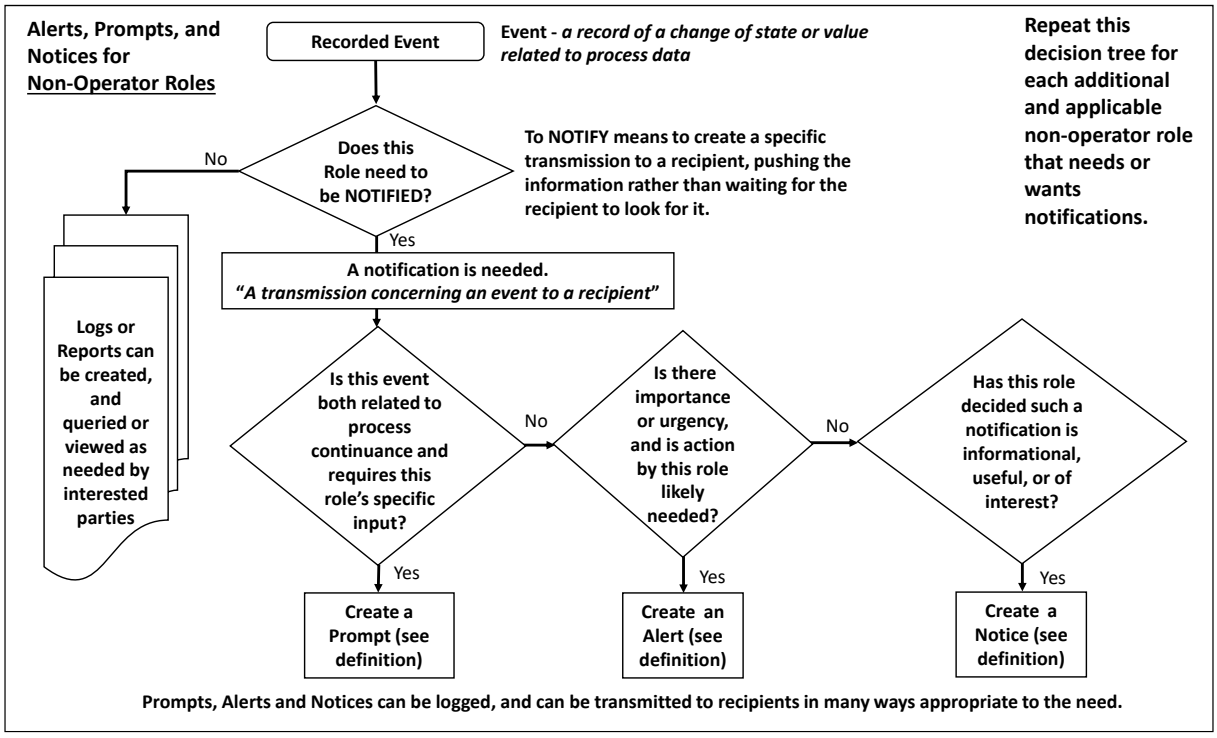

Figure 1 – Definitional structure for notifications for the non-operator roles

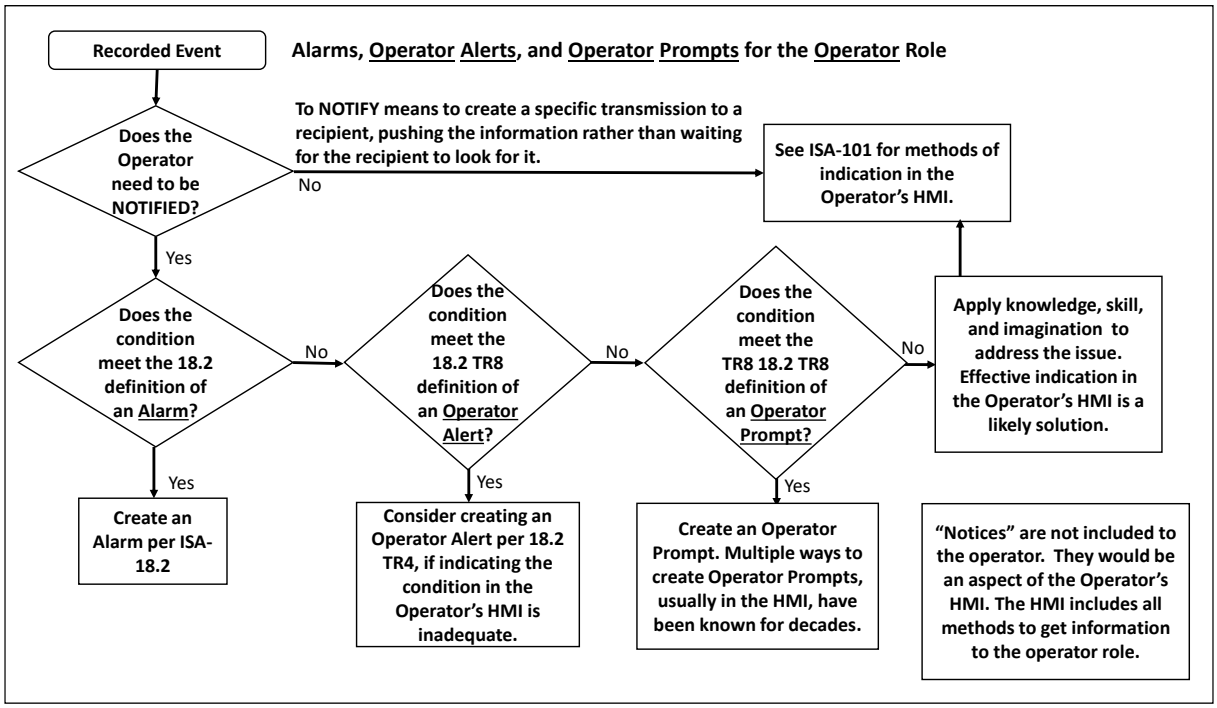

Figure 2 – Definitional structure for notifications for the operator role

4.2.1 Events

Event: record of a change of state or value related to process data

There are hundreds of types of events that can occur in a process facility and be detected by the process automation system. Events can also be created by people by using the automation system or systems connected or related to it. For discussion in this report, only events that are recorded and stored in some way are relevant, as only those can be further processed.

Various databases of different types of events are available for search and inspection. Some event types may be looked at frequently by different roles, others may never be looked at, or examined only as part of an incident investigation. Logic structures can look at various combinations of events and process conditions and create and record new events based on the results.

A recorded event can be processed in a variety of ways. In this TR, the first such way is to answer the question "Does someone need to know about this event?" If so, to notify means to create a specific transmission to a recipient, pushing the information rather than waiting for the recipient to see or go looking for it. In such cases, the event can be processed into becoming a notification.

4.2.2 Notifications

Notification: transmission concerning an event to a recipient

A notification is not "just" a "transmission of an event", it can have additional information that helps to put the event into context. The recipient is assumed to be a person and the characteristics of a notification need to be useful to the person receiving it. This TR is not about one form of electronic system communicating with another electronic system, although that may occur within this structure.

Notification is a word used to refer, in general, to the sub-types of alarms, prompts, alerts, and notices. In this TR, a recipient actually receives one of those subtypes of notifications, and not something designated only as a notification.

The method of transmission of any notification is supposed to be one designed to ensure the recipient becomes aware of them. This likely involves the nature of “pushing” something to the recipient. Simply placing an item into a searchable database is the nature of a “pull,” in which a person goes looking for information when they perceive a need. Push systems such as text messages, voicemail, email, and viewer systems (such as an alarm summary screen) are transmission methods that have a reasonable assumption that the recipient will become aware of the contents, particularly when the notification system is job or role-related, as is assumed in this TR.

The characteristics of the event and the intended recipient determine the type of notification and the method of transmission. A notification of a particular event might be defined and implemented as an alert to one recipient, a prompt to a different recipient, and even as a notice to another recipient.

Table 1 – Summary of defining characteristics of notifications

Notification type	Recipient	Nature of response
Alarm	Operator	Timely action needed.
Alert	Non-operator	Urgency of assessment and/or timely action needed by the recipient non-operator role.
Operator alert	Operator	Awareness or assessment with possibility of action for a condition not meeting all of the criteria for an alarm.
Prompt	Non-operator	Response needed by the non-operator recipient related to the continuance of the process
Operator prompt	Operator	Response needed by the operator related to the continuance of the process
Notice	Non-operator	Condition is of non-urgent interest to the recipient, but their action or response is not required

4.2.3 Notification sub-type: alarm

Alarm: audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a timely response

In coming up with the structure of this TR, alarms are obviously notifications, but with very specific requirements as to recipient and the nature of the event. Alarms are fully addressed in ANSI/ISA-18.2-2016.

In some cases, roles other than the operator may need or want to know about the occurrence of some alarms. It has long been possible in most control systems to route alarms to roles besides operators, and this is discussed extensively in TR4. In this TR, the terminology for accomplishing that would be to refer to such routing as being of alerts, prompts, or notices to those other roles, since alarms by definition go only to operators. While this statement might be true: “Our control system is configured to also send all Priority 1 alarms to the production engineer,” this TR would refer to those "routed alarms" as alerts or notices to the production engineer.

4.2.4 Notification sub-type: operator prompt

Operator prompt: notification to the operator related to process continuance that requires a timely response (e.g. task, data input, authorization, approval, permission to proceed)

This TR uses the term “operator prompt” for prompts addressed by the operator role, and “prompt” for those addressed by roles other than the operator. Generally, a prompt is a pre-programmed message with a variety of possible uses and responses. Prompts are often the concern of the operator but can be for other roles, particularly for authorizations. A prompt requires timely and usually specific response, or likely some aspect of the process will be delayed. ISA-106 specifically refers to operators as being the recipient of prompts. However, in many organizations, prompts are processed by other roles, particularly for such tasks as approving quality results and authorizing shipments.

Various methods to display prompts to the operator and to process operator responses have been used since the 1980s, generally via the operator's HMI.

4.2.5 Notification sub-type: prompt

Prompt: alert related to process continuance that requires a timely response (e.g. task, data input, authorization, approval, permission to proceed)

"Prompt" is the term used in this TR when the recipient and responding role is not the operator. Since the notification requires a response, and failure to do so likely delays the process and is probably considered urgent, a prompt is therefore also a (non-operator) alert, but with special characteristics.

4.2.6 Notification sub-type: operator alert

Operator Alert: audible and/or visible means of indicating to the operator an equipment or process condition for evaluation when time allows which could result in a response

The term Operator Alert has a significant history. The original ANSI/ISA 18.2–2009 defined it as "an audible and/or visible means of indicating to the operator an equipment or process condition that requires awareness, that is indicated separately from alarm indications, and which does not meet the criteria for an alarm." After IEC 62682 changes to the definition, 18.2-2016 revised it to an "audible and/or visible means of indicating to the operator an equipment or process condition that requires awareness and which does not meet the criteria for an alarm."

The definition of alarm is specific, containing several specific elements for a notification to qualify as an alarm. Alerts may only partially meet those criteria, therefore falling short of qualifying as an alarm. All of these versions defined "alert" as being role-based to the operator, but then provided little additional information about them.

Then, 18.2 Technical Report 4 provided much more detail as to how industry was differentiating operator alerts from alarms and using them effectively. In this TR8, the definition of alert is significantly broadened to include non-operator roles. To accomplish that without contradicting 18.2 and 18.2 TR4, TR8 uses the specific term "operator alert" to discuss the types of alerts mentioned in ISA 18.2, and 18.2 TR4. The guidance in TR4 still stands, just applying to the term "Operator Alert."

In general, operator alerts may or may not, meet some of the criteria for an alarm. They do not necessarily require operator action, or necessarily reflect abnormal conditions. An event that is useful for operator awareness but does not require specific operator action might be an operator alert. Advances in implementation of effective HMIs can also affect the use of alerts.

The lack of information about the use of alerts in the 18.2 standard itself led to some misunderstandings. The question has been asked, "In alarm rationalization, do all things that do not qualify as alarms become alerts?" The answer is "no," and that is supported by understanding the other sections of 18.2.

Consider this common situation. An unrationalized alarm system is full of "alarms" that do not meet 18.2 principles of definitions. These were the result of inconsistent use of alarm system capabilities, the lack of a consistent alarm philosophy, and years of inconsistent management of change. Applying ISA-18.2 rationalization principles results in the selection of some things that should remain as alarms, and many other things that should not be in the alarm system at all.

While 18.2 has a basic definition of alerts, it does not say that "everything that happens to be an alarm in an unrationalized system should be either an alarm or should become an alert." It has a section on alarms rejected in rationalization specifically addressing this. 18.2 intends that the alarm system is reserved for alarms, and then deals with the alarm system. 18.2 assumes that other methods are used to convey non-alarm information (which might include operator alerts) but does not go into detail on those. Historically alarms were often used as an adjunct or compensation to what we now recognize as ineffective HMI design. Subsequently to ISA18.2,

ISA-101 was published, discussing methods for creating an effective HMI. The selection and effective use of operator alerts was discussed thoroughly in TR4, after the original publication of 18.2.

4.2.7 Notification sub-type: alert

Alert: an urgent or important notification that may require timely response

This term is used for non-operator recipients. It is for notifications that the recipient would consider urgent, likely requiring their immediate attention, consultation, action, or response. The qualifier “may require” is used because the same alert could go to different roles (e.g., operations staff and plant management). In such an example the staff role is responsible to respond but the plant management or others are very interested in knowing about that urgent condition.

4.2.8 Notification sub-type: notice

Notice: a notification that is informational, useful, or of interest to the recipient

Notices are the “everything else” that do not have to meet the specific criteria to be prompts or alerts. They include important or simply useful information but are not considered urgent by the recipient, nor require a timely response from them. The phrase “worthy of notice” may be useful to evaluate whether something should become a notice. A notice should be significant enough to deserve a transmission, as opposed to the recipient’s looking up the information on an ad-hoc basis.

It is expected that the recipient of notices controls their ability to subscribe and unsubscribe from them at will.

The term “Notice” as defined in this TR8 is not applicable to the operator role. Process information needed for the operator role is implemented in the operator HMI. The term HMI refers to all methods used to get role-related information to the operator; it is not restricted to just control system graphic screens.

5 Events

5.1 General

Every active process environment includes physical or logical changes. These changes may be recorded as events that can be reviewed or interpreted by humans, devices, or applications.

As a basis for this Technical Report, events are interpreted as the superset and inclusive of all process condition changes.

This clause discusses events with and without notifications, sources of events, attributes of the event, and aspects of event routing.

5.2 Events with no notification

Some events have no need to generate notifications of any type. These can be valuable for troubleshooting and metrics reporting associated with process changes. For example, an operator makes a process setpoint change. This change is typically recorded as an event, but no notification is generated if the setpoint is normal, successful, and has not exceeded any boundary limits. Such setpoint changes can be used in statistical analyses or included in metrics for operator workload reviews. This setpoint change event can also be included in an incident investigation to include operator changes leading up to process upset.

To compare usage difference, the process setpoint change example above may require notification if the process change was not as expected. If the setpoint change, for example, was

not successful due to a control system communication error, then a notification may be required. Another possibility is the operator made a setpoint change that exceeded its prescribed boundary limits. These abnormal situations may require notification and the type of notification identified can depend on the recipient, process condition, or timeliness of a potential response.

5.3 Event sources

5.3.1 Event source types

Events can be generated from multiple sources. Process conditions are typically monitored and recorded by the automation system however other sources such as packaged systems, data historians or Manufacturing Execution Systems (MES) should be considered. The review, processing, and consumption of events may involve accessing multiple data sources and types for a given process area. Alternatively, the events can be consolidated and stored in a single location to provide a simpler access for intended recipients.

5.3.2 Control system

The most obvious event source is the control system. Depending on the use of the event, it can be recorded simply as a readable ASCII file or stored in a database. The information generated can show changes in logic, provide self-diagnostics, or record changes in process states.

5.3.3 Intelligent field devices

Field devices have intelligent diagnostics that can generate and archive events independently from the associated control system. These devices communicate events over standard communication protocols that allow dissimilar devices to provide not only process measurements, but also diagnostic and calibration events that are not usually seen by control system operators.

5.3.4 Handheld devices

Handheld diagnostic devices associated to field devices can generate events at the discretion of the user. Manual response to electronic checklists can be recorded and compared to process historian data. As an example, a checklist is a type of prompt. The persons performing the procedure can mark the steps on a list as they are completed.

5.3.5 Other systems

Other systems outside the control system can provide events that may or may not need to become a notification.

A local weather station, for example, may provide ambient temperature readings.

Internet web services can provide third party events that may be correlated with a change in process conditions.

Internal business infrastructure such as network monitoring and Manufacturing Execution Systems (MES) can generate events.

5.3.6 People

People themselves can directly generate events. With a compiled list of people-generated events, workload studies can be conducted to help identify process operations inefficiencies and adherence to procedures. For example, email or text messages are common modes to receive events that can be recorded easily. Voice phone traffic metadata from operators can also be logged as events to give information such as the start time, source phone number and call duration for Operations workload studies or notifications of important inbound or outbound calls. In addition, operator changes in manipulating the control system can be important events to be recorded for the same workload studies.

5.4 Event attributes

Events should provide enough information for the user to understand the change. As a basic requirement, the event should include the date and time of the event. Depending on the event source, the date and time may be shown with local time of the source or as Coordinated Universal Time (UTC). If the event date and timestamp are to be included in a notification, then the time could be adjusted to local time zone of the person receiving the notification.

The resolution and accuracy of the event data and time can also be important depending on its use. For example, event created in a Sequence of Events (SOE) recorder can provide valuable information in fault root cause analysis and requires the time to be recorded with millisecond resolution.

While not required, the event should provide the following information:

a) date and timestamp,

a) source (e.g., a device, field tag, etc.),

b) event type (e.g. attribute which gives distinction of the event),

c) description of the change (e.g., the previous and current states).

d) Importance of the event.

As mentioned in the event source discussion, events may come from multiple source types in a single plant location or site. It is recommended to review each source and attempt to harmonize and provide consistency in the event message format for all event sources. This allows dissimilar sources to be easily reviewed jointly and provide consistency for notification logic. When available, adding or modifying event attributes outside the original message format can provide the consistency desired.

5.5 Event routing and transmission

In this TR, an event is assumed to be recorded in some fashion. Even when the event does not become a notification, event routing may need to be considered. For example, events can be simply archived to an electronic collection, such as a file or database to be reviewed or used later for metric reporting or investigations. If events from multiple sources are routed and stored in the same event log, then data access and analysis may be easier.

Many event transmission methods and protocols are currently being used and new ones are being introduced every day. Technological details of transmission methods are outside the scope of this TR (see ISA95).

5.6 Event viewing

Control systems typically have a method to search and view all events. This is a mature technology, as such system vendors have been supplying and enhancing event historian search and view capabilities since the late 1980s.

6 Notification strategy

6.1 Development of a notification strategy

ANSI/ISA 18.2 applies a lifecycle approach to the management of operator alarms, where formal documentation and performance measures are required. This TR focuses on non-alarm notifications. Non-alarm notifications generally apply to less time-critical events and do not have to adhere to the same strict rules of ANSI/ISA 18.2. Exhaustive rationalization and consequence analysis may not be required. On the other hand, some of the lessons learned from the alarm overload problem can be applied to managing the massive volume of non-alarm notifications that can be generated by today’s automation systems.

Each facility may choose to develop a notification strategy that fits best with their existing work practices and information network. An important strategic decision is the degree of responsibility and reliance on notifications as part of the normal work. Some facilities may choose to rely on notifications as a form of job task list and to replace some informal types of communication. Others may rely on notifications for optimization activities that fill in the gaps in the normal work responsibilities. The strategy determines the effort and expenditure allocated for developing and maintaining the notification system.

A facility-wide notification strategy can result in a more consistent approach and more efficient use of available resources. Development of overall goals for the notification system helps to focus the efforts of the organization, resulting in a useful system that is easier to manage.

At the same time, a non-alarm notification system needs to transmit information to many recipient roles and should be customized to the needs of the roles. For best results, the recipient roles should be involved in all stages of development of the notification system. Each group may develop more specific and more detailed strategies and supporting goals.

6.2 Notification system work processes

Based on lessons learned from the alarm problems prior to ISA18.2, the intent of this TR is to avoid a potential “notification problem” by advocating good practices, without the requirement of a complex work process system.

Straight-forward characteristics for an effective notification system can be considered, such as:

a) notifications are timely, relevant, and useful to the recipients;

b) notifications are clearly worded and include sufficient information;

c) recipients are aware of how they should respond to notifications;

d) recipients know how to interact with the notification system;

e) recipient groups are involved in the design of the notifications intended for them;

f) recipients are not overwhelmed with too many notifications at one time (no flooding or chattering);

g) recipients are able to filter and sort the list of notifications based on defined criteria, such as source, importance level, area, or equipment type.

These characteristics can be the basis of the facility strategy to identify, design, and implement notifications and conduct periodic reviews to optimize the system. The specific methods, mechanisms, and frequencies can be determined by each facility or recipient group. This TR presents guidelines that may be helpful in these work processes.

6.3 Notification identification

6.3.1 Notification identification methodology

The goal of most non-alarm notifications is to improve efficiency and facilitate work. Thus, the process of non-alarm notification identification does not need to be as rigorous as identifying and rationalizing alarms. A systematic analysis, however, can be helpful to identify whether any and what kind of notification is needed. Recipient groups can identify the notifications that are useful to them in the performance of their jobs by analyzing possible event sources. Each event may generate multiple notifications to multiple roles or no notification at all.

Notifications can be identified by many methods, including those listed here.

a) During process design, prior to commissioning, notification types other than alarms may be identified that lead to improvements in operability.

b) During specification of major equipment or instruments useful notifications may be identified to non-operator roles. For efficiency, templates of typical equipment and instruments can

be developed, such that when new equipment of a particular type is specified, the notification requirements are already known.

c) When documenting the requirements for safety instrumented functions in a safety requirements specification (SRS), notifications may be identified.

d) As part of process review, notifications may be added to improve work processes and expedite decision making. For example, a notification may be used to indicate that an operation is deviating from its optimum conditions, while still within normal operating conditions. The notification provides an opportunity to adjust the process conditions so that they stay near optimum. Other notifications may prove helpful in general improvement activities, such as 6-sigma processes, operations excellence, and equipment reliability efforts.

e) During alarm rationalization process, the need for additional notifications may become evident. A notification that does not meet all the criteria for an alarm, as defined by ISA 18.2-2016, may be generated as other types. Alarms may also be combined with notifications to non-operators for the same event. For example, a failed instrument may cause an alarm notification to the process operator as well as an alert notification to the maintenance technician who needs to perform the repairs.

f) Facility's operation policies and procedures may necessitate notifications.

g) Notifications may be used to facilitate environmental or other regulatory compliance.

h) Notifications may be added as part of procedure automation strategy for the facility. Automated procedures may require multiple people to accomplish tasks during various steps. It may be helpful to prompt the recipients or alert them of any problems.

6.3.2 Events to notifications

Recipient groups can use their knowledge and experience to determine which notifications will be useful to them and what information should be included in the message.

The volume of collected events for process troubleshooting and analysis is often much larger than the required number of notifications. Additional, more specific data, or combinations of events may need to be captured.

A notification can be used to interpret multiple events into one concise and meaningful statement in less time that it would take for the recipient to sift through and analyze the events. For example, a "maintenance required" notification on a pump may be generated only if the pump has been running for at least 600 hours above 300 rpm. Pump status, speed, and accumulated run time may need to be stored in the process data historian.

Two different approaches can be used to make sure the required events are collected and monitored for notifications.

a) Identify the desired notifications. Then identify the events and process data that need to be captured to trigger the notification. In some cases, if the events are not already being recorded, responsible people or equipment vendors may need to be asked to add them.

b) Consider all the events that a device or an event source can generate, then select the ones that should produce notifications for specific recipient roles and add conditional criteria as needed.

Usually, a combination of both approaches is used. Items are monitored and collected by category. Exceptions are added as needed. Event generators can be grouped into similar categories to create notification templates. It will not be necessary to go through an exhaustive analysis every time an item from a category is added.

Large-scale, traditional BPCSs routinely monitor and record many events by default, such as all operator changes. In addition, process measurements are continuously collected in a historical database. Notifications can be triggered with relative ease from the collected data and events. In these systems, however, it is still necessary to choose among many available detailed events for monitoring and recording.

In many smaller control systems including SCADAs, every event and process data need to be particularly selected for monitoring and recording. Significant effort is often required to produce meaningful notifications from the events.

6.3.3 Event analysis examples

The following examples illustrate using event analysis to determine the different kinds of notifications to be generated.

These event lists are not all-inclusive. Roles that need to receive a notification type are listed under that column. Operator alarms and HMI are not discussed in this section. Any event may generate an alarm based on ISA18.2 and alarm philosophy. Visual indications may be included on the operator HMI based on ISA101 and HMI philosophy, independent of notifications. These examples intend to show how other notification types to other roles may be used instead or in combination. All events are logged with timestamp even if no notification is generated.

Table 2 – Event analysis example – equipment maintenance

Event generator: air compressor						
Available events	**Operator alert**	**Operator prompt**	**Alert to role**	**Prompt to role**	**Notice to role**	**Log**
Compressor failure – First-out			Compressor Maintenance Tech on call			Yes
Noisy vibration			Compressor Maintenance Tech			Yes
Primary serial communication to BPCS failed (auto fail-over to backup)	Yes		System Engineer, Compressor Maintenance Tech			Yes
Serial communication to BPCS recovered	Yes				Compressor Maintenance Tech	Yes
Low performance efficiency (calculated)	Yes		Compressor Maintenance Tech, Process Engineer			Yes
Perform routine maintenance (>600 hours)				Compressor Maintenance Tech		Yes
Compressor ready to start (standby)						Yes
Auto calibration complete (periodic)						Yes
Compressor Start/Stop (by operator)						Yes
Compressor setpoint change						Yes
Events 20 -60						Yes

654 **Table 3 – Event analysis example – procedural control**

Event Generator: Unit Startup Procedure Control Module						
Available events	**Operator alert**	**Operator prompt**	**Alert to role**	**Prompt to role**	**Notice to role**	**Log**
Perform field pre-startup inspection. Confirm.				Field Operator		Yes
Pre-startup inspection complete (confirmed)						Yes
Startup failure – problem (any of 20, First-out)			Field Operator			Yes
Auto valve stuck during startup			Field Operator			Yes
Instrument failure during startup			Instrument Tech			Yes
Startup took too long	Yes		Process Engineer		Operations Manager	Yes
Startup Successful					Operations Manager	Yes
Startup procedure started (operator-initiated)						Yes
Startup phase 1 complete						Yes
Startup phase 2 complete						Yes
Open manual valve in the field – Confirm to continue				Field Operator		Yes
Manual-valve-open not confirmed after wait time	Yes		Field Operator			Yes

655

656 **Table 4 – Event analysis example – process improvement**

Event generator: unit performance calculation module						
Available events	**Operator alert**	**Operator prompt**	**Alert to role**	**Prompt to role**	**Notice to role**	**Log**
Moderate drop in performance			Process Engineer			Yes
Significant improvement in performance					Process Engineer, Unit Manager	Yes
Significant drop in performance	Yes		Process Engineer		Unit Manager	Yes
Performance within expected range						Yes (trend data)
Invalid calculation			Process Engineer			Yes

657

Table 5 – Event analysis example – pipeline batch change

Event generator: pipeline batch change process						
Available events	**Operator alert**	**Operator prompt**	**Alert to role**	**Prompt to role**	**Notice to role**	**Log**
Batch Change Time Limit reached	Yes					Yes
Density Change Start		Yes		Field Operator – Adjust valves		Yes
Batch Change Complete			Inventory management			Yes

6.3.4 Notification database

Possible notifications can be documented in a database for consistency, reference, and training. A notification database could include the following attributes for each notification:

a) recipient role,
b) notification type (alert, prompt, notice),
c) algorithm or conditions for notification generation,
d) importance (for the role),
e) identifier (area/unit/equipment),
f) role-specific message,
g) method of transmission (specific to the role),
h) required actions (if any),
i) progress tracking (if any),
j) escalation path (if any), and
k) template type (if used).

The different fields can be specified by the recipient groups. Notification type and importance fields can be used to organize and filter the notifications. The wording and content of the message can be optimized to be meaningful to the recipients. The recipient groups can be trained on what to expect and how to respond.

If templates for device type or source type are created, multiple notifications with pre-determined attributes could be created automatically with the addition of a new event generator to the database. Message wording can include the identifiers for individual event generators.

6.4 Notification system design

6.4.1 Elements of design

Many of the alarm design good practices from ISA18.2 can be applied to notifications. Significant effort and analysis by each recipient group may be needed to design useful notifications from events. For example, slightly high temperature on a pump seal may not require a notification. But if the high temperature persists for a period of time and is accompanied by high vibration, then a notification could be sent to the rotating equipment specialist.

A common problem is that the manufacturers of automation devices and automation systems continue to call “events” alarms. After ANSI/ISA18.2 and IEC 62682 and this TR, they should be aware that the messages generated by default from the systems and devices are “events”.

Events may be used to generate notifications, including alarms, alerts, prompts, and notices by design.

Notifications of any type should be generated in ways that avoid problematic or nuisance behavior. ISA 18.2 and 18.2 Technical Report 3 specify methods (e.g., deadbands, delay times, debounce timers) to avoid chattering and fleeting alarms. Similar practices to avoid such problems can be applied to the generation of notifications.

The following is a list of possible steps in designing a notification system to support a facility strategy.

a) Identify criteria for notification generation.

b) Make sure the required events are captured.

c) Develop pre-registration templates for known types of event generators (device, equipment, process, or procedure that can generate one or more events).

d) Develop consistent message format for recipient roles.

e) Determine method of annunciation and display on the recipient user interfaces.

f) Determine the mechanism to assign individuals to a specific recipient role at any particular time.

g) Determine how to implement escalation rules and determine transmission paths, if part of the strategy.

h) Determine the method of capture of acknowledgments, actions, or completions, if part of the strategy.

i) Determine requirements for user access and cyber security policies.

j) Determine how to handle user opt-in and opt-out of notices.

6.4.2 Notification message

An event message may be modified or enhanced with recipient-specific information to make it into a meaningful notification. Attributes such as source identifiers, importance, possible impact or required action may be added to the original event message as determined by the recipient group. Notification message formats may be specific to the type of notification, equipment, or site, and should be consistent as much as possible.

6.4.3 Notification infrastructure

In a traditional BPCS, the data processing, event generation, and notification were performed by the BPCS equipment. In today's, more open, automation systems, these functionalities can take place in equipment anywhere within the network, such as supervisory control servers and process information management systems (PIMS).

Notification systems depend heavily on the information networks at the facility. In addition to functional requirements, reliability and capacity of the network will need to be considered. Issues such as server redundancy, database storage integrity, communication speed, network security, and local and remote user access should be included in the strategy.

Delivery mechanisms need to be tailored to the strategy requirements. Some providers of text messaging (SMS), for example, do not warrant delivery of the message or the delivery time. When guaranteed delivery is required, appropriate delivery service should be employed.

6.4.4 Time-critical notifications

The facility may decide to use the notification system to send alerts that require timely response to on-site or remote personnel that are not control room operators. In that case, the notification strategy needs to include additional sections to discuss these requirements. The notification communication system and user interfaces may need to be more robust. The recipients should

be trained to respond appropriately to these notifications. Acknowledgement and escalation strategies may need to be included.

6.4.5 Notification documentation and training

A notification strategy can determine the level of documentation and training required. Notification management may be incorporated in the existing facility work procedures or in a separate document. Each recipient group may also develop a group notification strategy document if the work procedures are deemed complex enough. The documents can be used for training new group members and to maintain consistency on notification management.

A facility may decide to apply to notifications some of the techniques developed in ISA18.2 Management of Change (MOC) for alarms. MOC ensures that changes are documented with appropriate authorization and personnel involved are trained before implementation. The degree of documentation and authorization may be defined in the notification strategy.

6.4.6 Notification history and viewing

A capable means for searching, filtering, and viewing alarms and events is a common feature of control and automation systems. Similar means to accomplish similar searches on notifications are desirable.

6.5 Notification system implementation

Implementing a facility-wide notification management system can be more complicated than the operator alarm system. The non-alarm notification system involves many parts of the facility's information infrastructure and communication by means of various user interface devices. Notification implementation system should satisfy the needs of all recipient groups.

Implementation of the notification system can be phased in gradually. For example, initially, all notifications to a recipient group can be sent to a central access point, where they can be viewed by multiple people. Individual recipient user interfaces can be added at a later time. Also, different recipient groups can be phased in one at a time. Feedback from the system for acknowledgement/confirmation and escalation can be added in later phases if required.

Historical databases of notifications can be made available to authorized personnel for searching, filtering, viewing, and generating reports. By the definitions in this document, the review of the historical database or reports is not considered being notified since the information is "pulled by" and not "pushed to" the recipients.

Many PIMS, currently available on the market, provide tools for routing notifications to various recipients. PIMS routinely collect alarm and event logs from the automation system. Software configuration allows communication of the events to assigned recipients based on defined criteria. Other products help manage user access rights to the facility information network and the individual user interface devices. This TR does not endorse any particular software product.

Regardless of the transmission mechanism, the notification strategy can define the requirements for the implementation system, such as the following:

a) required events are captured,

b) notifications are routed to the right recipient,

c) required attributes (type, importance, etc.) can be added to the original event,

d) message format and wording can be customized for the recipient groups,

e) acknowledgement/confirmation and other response requirements can be added as needed,

f) escalation is available if needed,

g) notification creation is allowed by users at various authority levels, and

h) opting in or out by a recipient is possible.

Each recipient group should develop the requirements and be involved in the design of the notification system for their group. Configuration and programming of the software product can be sourced outside of the group as multiple entities may be involved, within and outside of the facility.

6.6 Review and optimization of notifications

A notification strategy may include guidelines on the review procedures and frequency to keep the notification system efficient and useful. Any change to the automation system that impacts event generation may require an update of the notifications. For example, if an instrument manufacturer updates the model of a flow transmitter, the list of available events for the device type should be reviewed and the notifications to the instrument technicians modified as needed. Changes to role assignments may also impact notifications.

Any existing notification system should be reviewed periodically to make sure the strategy guidelines are followed. The following items can be checked to optimize the system

a) Make sure the notification is still needed. A notification may have been added during new process start-up or for troubleshooting and is no longer needed. Alternatively, limit the notification to specific process phase, such as during start-up only.

b) Duplications should be avoided. If the recipient receives multiple notifications for the same event, combine into one.

c) Make sure the notification goes to the right recipient. If the designated recipient does not have control over or skill to respond to the notification, reassign to another recipient. Limit distribution to those directly responsible.

d) Make sure the notification is the correct type. For example, if the notification is implemented as a notice to the maintenance function that requires a fast response, it should likely be an alert instead. Also, some alerts may have been mis-categorized as such to reduce the number of operator alarms and they should be re-evaluated.

e) Make sure the notification reaches the recipient. If the designated recipient is too busy or out-of-area temporarily and cannot respond to the notification, add alternative or escalation path.

f) If the required action as the result of the notification can be accomplished automatically by the automation system, configure automatic action, and only generate notification if action is not completed within a reasonable time.

g) Eliminate chattering notifications. Repeated notifications for the same event should be avoided.

h) If the notification is only generated for possible reference at a later time, consider deleting it. This can be recorded as an event or in a report. Consider replacing the notification with a status change (color, symbol, text) on the HMI or user-interface. For example, in batch processes, events are often generated to capture time stamps of various tasks for the batch report, but not all these require notifications.

7 Alerts for non-operator roles [Hollifield]

7.1 Purpose

Automation systems have become capable of generating notifications of interest to a variety of roles other than the operator. In the past, many such notifications were implemented as alarms, with the expectation that the operator would relay the information, posing an unnecessary load and affecting the performance of the alarm system. Since automation systems are now capable of sending notifications directly to the appropriate recipients, this section discusses several possible non-operator roles and the nature of alerts that could be of interest, with examples.

Operator Alerts are then discussed based on the contents of ISA-18.2 TR4, with additional information.

7.2 Alert message characteristics for non-operator roles

Alert messages should be tailored to the recipient roles. Equipment designations and the terminology used should be easily understandable to the recipient. Additional training may be required to ensure the recipient of the alert knows how to interpret and handle it.

In some cases, non-operator alerts could be tagged with words, symbols, or fields indicating their relative importance, category, or type.

Alerts may require actions within a specific time. The alert message design could include information on what might happen if the response actions are not completed within a given time, and whether escalation to a different recipient could occur for this particular alert.

7.3 Operator alarm vs. non-operator alert speed of response

The “timely response” aspect of the definition of an alarm is partially based on the nature of the operator role. Alarms are communicated via the operator’s HMI, which has an expectation of being manned, often on a 24/7 basis Non-operator roles are usually not manned 24/7 (although exceptions exist at some sites for some roles.) People in non-operator roles are not generally expected to need to immediately detect and respond to an electronic message. An individual working a normal work week, including long weekends and vacations, cannot be expected to make a response of the same nature as the “timely response” phrase used to describe alarms.

In cases where there is need for a response that is not delayed by up to several days, companies use practices such as staff-on-call, “weekend duty,” pagers, or similar methods to ensure a staff member is available to respond to a communication from the operator or plant.

In some ways, communicating alerts to non-operators can be more complicated than alarms to operators. While alerts are sent to the designated recipient roles, this may not involve a fixed location or even a fixed specific device. A login account accessible from many different devices could be used.

Recipients can receive alerts on the specific user interface device(s) and application software determined for the role. The recipients should be able to sort/filter the alerts and other notifications based on various criteria.

If acknowledgement of the alert is required, the recipients need to be able to communicate the acknowledgement through the same user interface device. Acknowledgement would be recorded as an event, confirming that the recipient has been made aware of the condition. In some cases, if acknowledgement is not received from the designated recipient within the allowed time, escalation processing could forward the alert to the next recipient on the list.

Quick responses may be required by some alerts. In some cases, the recipient may need to follow a set procedure (defined steps) to complete the actions. The recipient may need to wait for others to complete certain steps before proceeding. If the facility uses a procedure management system (see ISA 106), completion of each step may be recorded as an event through a checklist. Additional prompts or notices may be involved. Notification strategy of the facility may define the required information that needs to be captured and communicated.

Sections 7.4 through 7.15 present examples of various recipient roles that may receive alerts, and the potential nature of such alerts.

7.4 Alerts for production engineering and supervisory roles

These roles are typically site or unit based, and responsible for the efficient day-to-day operation of a process. These roles may be involved with process improvements, such as representing production interests on capital project teams. Alerts for such engineers and supervisors could be based on a variety of process-related issues associated with safety, quality, efficiency, and productivity. For example, a process excursion that fails to meet

efficiency or production goals by either a certain magnitude, or for a predetermined period of time, might generate an alert.

Production engineers may also specify and run tests on the process to measure the effect of different control strategies, newly-commissioned improvement projects, equipment changes, or other modifications. Since such tests may run 24/7, alerts can provide valuable information without the need for the person to be on-site. Alerts could similarly be based on the process attaining (or failing to attain) certain goals during off-hours or weekends.

7.5 Alerts for process engineering roles

This role is often associated with a central engineering group, involved in the design and improvement of a process. This role may be involved in plant design and commissioning, but not assigned to a unit once in production. However, periodic monitoring of the unit's performance is often a responsibility of this role, as well as verifying design assumptions and identifying potential improvements. The use of a process historian is common for this role, and alerts based on pre-determined conditions may also be useful. It could be that alerts to the production staff based on process performance might be considered notices to the Process Engineering role, if urgency or timely response by that role are not required.

7.6 Alerts for instrument and equipment maintenance roles

In some cases, the only action an operator takes regarding an alarm is to initiate a maintenance work action. The control system may have the ability to route such occurrences directly to the appropriate place in the maintenance organization for work initiation, thereby making them alerts. This can unload unnecessary alarm traffic from the operator. Typically, these would be alerts related to malfunctioning equipment or field devices needing technician attention.

It may also be possible that equipment can generate notifications of needed maintenance in other ways, some of which may have longer time horizons than those typically specified to qualify for an alarm, and should not be implement as an alarm.

It is possible that some alerts could be configured that would require quick response from a maintenance-related role and would need to use a method involving on-call procedures.

7.7 Alerts for automation system maintenance roles

Control system engineering or similarly-named groups are often responsible for the complex inner workings of the automation systems. These groups could be the recipient of alerts related to internal diagnostics of the control system itself. This would be for items that are not suitable for resolution by the operator.

Some such reported internal conditions could be handled on a routine basis. Others could indicate a condition that would require quick response from a systems-maintenance-related role and would need to use a method involving on-call procedures.

7.8 Alerts for reliability engineering roles

Complex machinery may be monitored by engineers or technicians specifically concerned with reliability. This role may desire alert generation based on complex combinations of time in service, load, or other factors related to the machinery.

7.9 Alerts for environmental administration roles

It is common for plants to have emission or discharge limits that are not instantaneous but based on totalized time-weighted averages or similar methods. Alarms suitable for the operator to take action to avoid those limits may not use the complex calculations needed for emission compliance reporting. Alerts for that purpose could be created, with the recipient being the role responsible for reporting environmental compliance and non-compliance.

7.10 Alerts for production department management roles

The first-level manager of a production department or plant may have concerns related to areas monitored by several different production engineers or supervisors. Additionally, this manager will have interest in non-routine maintenance needs that might be detected by maintenance or reliability functions, as well as those associated with environmental monitoring. Alerts can be customized for that role in a manner that does not simply duplicate those received by subordinate or support functions.

7.11 Alerts for site management roles

A site manager with several production departments may desire alerts that are similarly constructed and customized based on combined performance of the production departments making up the overall site.

7.12 Alerts for executives

Corporate executives responsible for several sites or regions could desire alerts based on overall single-site performance, or the aggregated performance of several different sites in different areas, such as production performance by product line.

7.13 Alerts for roles involved in cybersecurity

It may be possible for the control system or ancillary connected equipment to monitor for issues related to cybersecurity. These could include such things as invalid login attempts, unauthorized management-of-change of embedded software, or suspicious network traffic.

Alerts related to such events might be routed to a variety of roles, but particularly to a role monitoring cybersecurity. The response would likely be to engage the production department at the managerial or engineer level, or to engage the control system engineering function for further diagnosis.

When a cybersecurity alert is first generated, it is likely that the cause and potential consequence are not definitively known. A first step might be to perform some level of analysis and forensic investigation to evaluate whether the alert represents a non-incident, a cybersecurity incident or a non-cyber security incident.

Cybersecurity alerts are typically not routed to operators, but instead should be sent to control system administrators, control system engineers, security experts, or other personnel that can perform the necessary investigation and evaluation. Communication of cybersecurity alerts should use terminology familiar to the recipient.

Examples of potential cybersecurity alerts include the following:

a) Maximum number of failed login attempts exceeded
b) Failed connection attempt between the business network and control system network
c) Anti-virus software has detected malware on control system (operator stations or engineering workstation)
d) Disabled anti-virus software or other security controls
e) Unusually high network traffic or unknown traffic from external network
f) Intelligent field devices connecting to outside Internet Protocol (IP) addresses
g) Firewall error
h) Unknown or unexpected firmware pulls or pushes

7.14 Alerts for roles concerning safety instrumented systems

Alerts from a Safety Instrumented System (SIS) can be used to communicate equipment faults, functional status, or diagnostic information that does not require specific timely action by the operator. As appropriate, these notifications can also be sent to maintenance and engineering roles individually or in combination with the operator. Operator attention and action related to SIS alerts may be important to achieving the claimed risk reduction for a safety instrumented function (SIF), especially where diagnostic credit has been taken for the operator recognizing SIS mis-operation and taking corrective action. Such conditions are likely implemented as alarms.

SIS alerts may require periodic testing and the creation of response procedures depending upon the targeted role. Requirements for SIS alerts should be identified during the design and engineering phase of an SIS and should be documented.

Possible examples of alerts issued by the SIS include:

a) Indications related to support systems for the SIS that are not required for the SIF and where there is sufficient time to detect the support system failure prior to the dangerous failure of the SIS (e.g., climate control, heat tracing, purges).

b) An SIS diagnostic that is relied upon to indicate a % of safe or dangerous failures during SIL Verification calculations could be an alert to an engineering group.

c) Device failure that decreases the availability of a safety instrumented function from a 2oo3 to a 2oo2 or 1oo2 vote to trip. If the device failure results in a reduced safety Integrity level (SIL), then it could be an alarm if interim procedures are used in that circumstance. If there is no change to SIL, then the device failure could be an operator alert or a maintenance alert.

d) SIS Proof testing status when manually initiated per documented test procedure. Notification that the proof test is active could be an alert sent to the operator and maintenance, although personal communication between the tester and the operator is a common method that guarantees awareness. Indication of a failed test could be a maintenance alert to indicate a need for action. If the test is successful a notice could be sent to maintenance indicating no action (other than recordkeeping).

e) SIF Bypasses annunciated to the operator and maintenance (e.g., Bypass active, Bypass has been active too long in relation to mean time to repair). It is common practice to have SIS maintenance bypasses as alarms to the operator when defined accordingly in the alarm philosophy.

7.15 Operator alerts

7.15.1 Introduction

ISA-18.2 defined alarms in terms of the operator role. It then put everything “non-alarm” into the category of an alert, defined that as follows (still in terms of only the operator role), and did not address use of alerts in the standard.

The 18.2-2009 definition was:

“An audible and/or visible means of indicating to the operator an equipment or process condition that requires awareness, that is indicated separately from alarm indications, and which does not meet the criteria for an alarm.”

In the development of IEC 62682, the definition was modified to be less specific:

“audible and/or visible means of indicating to the operator an equipment or process condition that can require evaluation when time allows.”

Then, as part of harmonization with IEC 62682, the 2016 version of ISA-18.2 changed to this definition:

"audible and/or visible means of indicating to the operator an equipment or process condition that requires awareness and which does not meet the criteria for an alarm."

The commonality of these definitions is that alerts are only defined for the operator role. No content about alerts was included in any of these three documents. The implication is that alerts are separate from alarms.

This technical report now defines operator alert as an audible and/or visible means of indicating to the operator an equipment or process condition for evaluation when time allows which could result in a response. The intent is that alerts may, or may not, meet some or any of the criteria for an alarm. If all of the criteria for an alarm were met, the condition would qualify to be an alarm.

ISA-TR18.2.4-2012 Enhanced and Advanced Alarm Methods (TR4) included a detailed chapter on how industry is effectively using alerts. The chapter contents primarily dealt with alerts for the operator role.

When this Technical Report 8 was initiated, the scope decision was made to expand the definition of "alerts" to cover roles other than the operator. Therefore, the term "operator alerts" is used in this document to refer to alerts as defined by either ISA-18.2 (2009 and 2016) or IEC 62682.

Following is an abridged and slightly modified summary of the information in TR4 on operator alerts. Information about alerts for roles other than the operator is omitted since that is covered previously in this section. The full TR4 is recommended.

7.15.2 Problems and opportunities for operator alerts

For an effective alarm system, it is important to have a clear distinction between alarms and operator alerts. This clause describes the overall function and rationale for an operator alert system, that is distinct from the alarm system.

Modern control systems often have considerable functionality for generating a wide range of events, operator notifications, and log entries. This section deals only with those that pertain to alerts intended for the operator role.

Challenges involved in establishing an alert system for the operator role include:

a) the need to ensure an unmistakable distinction between operator alerts and alarms, such that the engineer designing the alarm (or operator alert) system and the operators share a common understanding;

b) the need to segregate operator alerts such that they do not have potential to compete with the operator's focus on active alarms;

c) the need to provide an operator alert system useful for purposes that do not qualify to be an alarm.

The site alarm philosophy document should specify the means for differentiating between alarms and operator alerts.

7.15.3 Example alarm philosophy treatment of operator notification

An example of how operator notifications could be defined in an Alarm Philosophy is shown in Table 6. This example describes how each notification type is represented in the HMI design.

Hence it provides clarity relative to notification cause and the expectation of an operator action, removing any confusion on the part of control system designers and users.

Table 6 – Sample criteria for notification types from an alarm philosophy

Operator notification type	Example notification text	Comment
Alarm	High level in Tank 26	This is an alarm because operator action is needed to prevent the tank from overflowing.
Operator Alert	High reference impedance. Potential cause is coated PH probe.	This could be an alert to the operator, assuming the pH reading to the operator is still valid. It might be routed directly to the maintenance function, If the reading has become invalid, the operator should know that, likely via an instrument diagnostic alarm.
Operator Alert	Tank level at 67%; stop transfer to leave adequate material for tomorrow's shipment.	Though operator action is required to avoid a consequence, it is not an alarm since it is part of normal operation. Also, the temporary setting or resetting of an alarm to provide the indication is often impractical due to alarm system management-of-change practices and considerations.
Operator Prompt	Notify quality lab that batch is ready for sampling. Initiate and maintain hold cycle until receipt of disposition notice/release approval.	This is not an alarm since it is part of normal operation and is not an abnormal condition. It does require an operator action associated with preventing further processing.
Operator Prompt	Verify ready to proceed to recipe blending phase.	This is not an alarm since it is part of normal operation and is not an abnormal condition.
Operator Alert, or Equipment Status shown on HMI	Compressor start-up sequence moving from purge to start-up.	No operator action is required, only operator awareness. Note it may be more effective to simply depict the sequence position and status in the HMI, on the graphics used by the operator to monitor compressor startup.

7.15.4 Operator alert system characteristics

An operator alert tool creates alerts that are not presented to the operator as part of the alarm system, and operator alerts are not mixed in with alarms. Operator alerts fall outside of the alarm priority-setting methodology and should have their own separate audible tone, iconic representations, color use, rules for symbology, etc. Operator alerts should not appear on the alarm summary display. Often there is a similar type of display showing alerts that are in effect.

The operator should be able to create and delete some alerts at will. Note that the operator may not be allowed to alter certain engineered alerts provided, for a variety of reasons.

The alarm system is intentionally designed to be an interruption to the operator, with known tones and behavior. Therefore, the initial indication to the operator should not be identical for an operator alert as for an alarm.

The intent of these restrictions is to ensure that any notification from the operator alert system is of lesser importance than an alarm. Thus, the proper operator action is always to deal with alarms before operator alerts. During high alarm-rate situations, the operator alert system is of lesser priority than the rationalized alarms. Dealing with the alarms will avoid more significant consequences than will occur from missing an operator alert.

Note that the depiction of equipment status, state (e.g., running or stopped), or condition in an operator's HMI is not a "notice" under the definitions of this document. Operator HMI displays are the subject of ISA-101.

7.15.5 Commercially available operator alert products

Alert products for operators first reached the market from 3rd party suppliers, not BPCS manufacturers. The capabilities described in this section have grown over time and become popular with BPCS users. More recently, some BPCS vendors have begun to expand BPCSs to include operator alert capabilities of varying capability.

Commercially available alert software exists to provide a separate alert system for use by operators, engineers, and managers. This requires a data connection to the process.

A useful operator alert system may have the following desirable capabilities, based upon user feedback:

a) Present alerts in an interface separate from that of the alarms.

b) Create alerts based on analog, digital, or logical process values, singly or in combination, and including timers.

c) Allow user-configurable, user-controllable alerts.

d) Allow for individual operator, engineer, or group accounts (e.g., “B” Shift) for separate sets of alerts.

e) Allow for alerts that are mandatory for selected accounts and that cannot be changed other than by administrator access.

f) Allow for controlled alert suppression e.g., “alert shelving”

g) Have audible annunciation that is different from alarms, and capable of volume adjustment.

h) Have visual characteristics that are different than the control system presentation of alarms.

i) Allow for sending of pre-determined alerts by email or text message.

Alerts can be model-based or rule-based. Alerts can be crafted to give the operator advance warning of potential abnormal situations, for review and action.

While some tools allow for different priorities of operator alerts, this is generally seen as an unnecessary complication.

7.15.6 Operator alert effect on alarm rate KPIs

ISA-18.2 contains a variety of alarm-related KPIs, such as recommended maximums for alarm rates. A separate alert system does not affect those KPIs, since by definition alarms are more significant than alerts and the intent is to always give alarms precedence over alerts for response.

It may be useful to analyze the occurrence of operator alerts in combination with alarms, particularly for operator alerts that cannot be altered by the operator.

8 Prompts

8.1 Nomenclature

Prompts concern normal and expected aspects of the process, at which point human confirmation, data input, authorization, approval, or similar action is needed to allow the process to continue. The term “process” should be considered in the broad sense.

As an example, shipping a product is part of an overall production process, and may require confirmation or signoff by a person that certain lab tests are satisfactory. An automated prompt generated upon the lab work’s completion can be used to initiate such confirmation, allowing the shipment to proceed at the earliest time.

This TR defines both operator prompt (for the operator role) and prompt (for the non-operator role.) These are separated because of the specific nature of the operator role, which has other applicable standards such as ISA-18.2, ISA-106, and ISA-101. In some cases, there are regulations concerning the operator role specifically, which are not applicable to other roles that may also receive and respond to prompts.

8.2 Operator Prompts

Prompts have been commonly used for decades to assist operators in performing a variety of tasks. As an example, equipment that is started or shutdown infrequently may have programmed routines that guide the operator through the operation in a safe and efficient manner, rather than simply relying on written procedures or checklists. These routines may have several steps that require the operator to confirm that certain actions have been taken, actions that cannot be sensed by the automation system. Such steps would be considered prompts, as they are normal and expected aspects of the process.

Any methodology that is provided for the operator to interact with the process is considered as per of their provided human-machine interface, and is therefore part of the subject matter and guidance of ISA-101. Various methods to display prompts to the operator and to process operator responses have been used since the 1980s, generally via the operator's HMI.

8.3 Prompts for roles other than the operator

Many roles other than the operator may need to interact with the automation system. Some of those interactions will meet the definition of a prompt, in which the event is expected, a specific response is required, and failure to provide one likely delays the process.

These roles will likely receive and respond to prompts via their office or portable computer, or portable device. Such devices do not meet the definition of an HMI as used in ISA-101, so the mandatory aspects of that standard do not apply.

The previous recommendations and guidance around alerts for the non-operator role are relevant to prompts as well.

9 Notices

9.1 Introduction

The clause concerns the notifications not meeting the criteria to be an alarm, alert or prompt.

9.2 Use of notices

Notices are notifications that do not require a response by nor immediate awareness of the recipient. They are intended to make the recipient aware of an event, state change or combinatory logic (e.g., sequence of events, combination of event and state, combination of trend and state change, KPI threshold excess, etc.) he is interested in or configured by the recipient.

For the operator role, events that are not alarms, alerts, or prompts, may be displayed visually (symbol, color, or text) on the HMI displays as status changes following ISA101 guidelines.

For non-operator roles without access to the operator HMI, a notice serves the purpose of bringing an event, that is not an alert or a prompt, to the attention of the recipient. It should be possible for such roles to subscribe and unsubscribe to various notices that they find useful, and have notices created or modified to serve their needs, if the technology allows.

Methods described under Notification Strategy should be employed to avoid over-use of notices.

9.3 Examples of notices

9.3.1 Equipment selection

A central process engineering design function may evaluate and decide to choose previously untried equipment in the process. Once the process is in operation, that group may want to monitor its performance, to verify design assumptions and validate the choice. This monitoring could include both process historian information regarding performance, as well as notices generated specifically for the design group.

The same could apply to local engineering functions, or even equipment modifications designed and installed by production resources.

9.3.2 Production planning

A production planning function is interested in meeting demands for multiple products, often produced on the same equipment, involving scheduling of that equipment and close monitoring of rates and inventory. Notices associated with how daily or weekly production is matching the overall plan can be useful to that function.

9.3.3 Production management

All levels of production management are concerned with productivity, yield, conversion, and efficiency. Different managerial levels could benefit from notices regarding performance indicators that are tailored to their specific needs (e.g., local production unit, similar units at different sites, plant, or regional performance).

9.3.4 Boundary management

Automation systems can generate notices tailored to informing management of any excursion of the process into undesirable regions of production rate, efficiency, emissions, yield, quality, or other parameters. Solutions for automated detection, analysis, and reporting of such excursions exist.

10 Notifications user interfaces and considerations

10.1 Nomenclature

While human-machine interface (HMI) is a generic term in industry, ISA-101.1-2015 defined it as

> *"the collection of hardware and software used by the operator and other users to monitor and interact with the control system and with the process via the control system."*

Then, the content of ISA-101 concentrated almost exclusively on the operator role and particularly on process graphic representations for use by the operator. The design of an operator's HMI was not to be compromised for the occasional use by other roles. Mention of non-operator roles in ISA-101 still concerned the operator's process control domain. Some aspect of the operator's HMI would be assumed to be the method of transmission of notifications to operators, and the principles in ISA-101 would apply to those. ISA-101 did not go into detail on user interfaces for non-operator roles.

Much of the design of ISA-18.2 and ISA-101 reflected an assumption or strong possibility of 24/7 job coverage by the operator and the need for quick, real-time detection and response to process conditions. Unlike the operator role, time sensitivity may not be a factor associated with a non-operator role's use of some notifications. The transmission of notifications to such roles may use a variety of hardware and software.

10.2 Methods of notification transmission and indication

For non-operators, notifications are likely to be received using the same conventional hardware and software used for the remainder of the recipient's job. This may include:

a) Email, text messaging, or similar messaging applications.

b) Event viewer or dashboarding style applications, including web pages.

c) Customized user interfaces based on database query tools.

d) Use of portable devices (e.g., laptops, phones, tablets).

e) Browser-like applications that access a company's internal network.

f) Customized interface creation associated with applications such as process historians or alarm management systems. Some such applications provide flexible capability to design screens for viewing process data in near-real time, including the ability to define, create, and transmit notifications of various types to predetermined users.

Users will expect that they will receive alerts in a user interface that follows standard display and interaction conventions used by common productivity applications on the relevant hardware platform.

10.3 Key performance indicators for notifications (alerts, prompts, and notices)

10.3.1 This is a hanging paragraph

ANSI/ISA 18.2-2016 and its technical reports discussed a variety of key performance indicators for alarm systems. Performance analysis was necessary, because it was common that alarm systems were configured to present thousands of alarms a day to a single operating position. In such a case, a system that was essential to the operator's work responsibilities, but over which they had no ability to control, became a nuisance distraction or even hindrance to their job, and ultimately to the performance of the process. Detailed analysis of alarm system performance is a necessary step for improvement.

The situation is different for the notifications (alerts, prompts, and notices) discussed in this TR. The practice of copying and routing alarms to non-operator roles for various informational purposes is covered in TR4.

10.3.2 Roles differences

This TR's subject includes roles that are not performed 24/7. Staffers with typical 40-hour or similar work weeks will be recipients of different types of notifications. Various means of transmission will be used for such roles, such as viewer applications, texts, and email. Unlike the operator role, there may be little to no time sensitivity associated with a role's use of some notifications.

In general, users of notifications may view them (on demand) as needed through the use of a viewer-type application, or may subscribe to some notifications in order to receive them through email, text message, or similar means. The user chooses to view or subscribe to some notifications because of their usefulness to that job role. The user has control over what they choose to look at or to receive. If certain types of notifications are not useful for a job role, that role can cease to view or receive them. This is fundamentally different from the alarm system problem.

10.3.3 Measurement of notification generation

Analysis of some notification types may be very useful to a job role, similar to the practice of determining the most frequently produced alarms in a process. Notification systems may include the ability to produce such analyses based on the recipients need.

The question might arise – "Are there any recommended performance numbers or limits for notifications sent to a non-operator role?"

There is no human factors research to rely upon to determine any recommendations for maximum amounts of notifications useful to a specific job role. For that reason, this TR does not contain any such recommendations. It is the recipient's responsibility to ensure their selected volume of notifications supports their work requirements. It is the notification system's designer's responsibility to ensure their design is useful to the roles they serve.

Here is an analogy. While email may be one way in which a job role obtains notifications, there are significant differences between notifications and email. Almost anyone can push an email to any other person. The recipient has little control over what is received. While there are the abilities to block senders or domains, and set up rules and spam filters, these are after-the-fact and often work poorly. Even with this being a world-wide problem, there are no KPIs such as "how many emails per day are too many?"

In some industries, overall workload analysis of some roles may be desired, which could include alert generation rates.

10.4 Avoiding notification overload

Today's highly networked automation systems make it very easy to generate many notifications to many recipients. In the spirit of ISA18.2-2016 and ISA101-2015, notifications should be task-related and targeted to the appropriate recipients, and should be added by-exception-only to limit information overload and distractions. The recipient of the notification should have control over the information they receive.

11 Case studies

11.1 Case study examples

The following case study examples are presented to illustrate effective use of notifications by various recipient roles.

11.2 Instrument group notification template – Coriolis mass flow meter

The Instrument Group in a facility reviews the vendor-provided events list for each type of instrument and decides which ones can provide useful notifications for their group. The group then assigns the type of notification, importance level, and a description of event that is meaningful to their group.

To expedite their analysis, the Instrument Group assigns a notification template to each type of instrument. When a new instrument of a known type is added, the notification decisions have already been made. Instrument Group's notification database consists of the templates for all instrument types and a cross-reference list between the existing instruments and templates.

In this example, the template Flow_Crls_01 is used for a Coriolis flow meter. The Instrument Group has decided to receive notifications from a subset of events as listed in Table 7. (The failure events may also be designated as possible alarms to the operator, not discussed here.)

In this example, the vendor has supplied a "severity code" for each event. The severity for the event is based on the individual instrument type. The Instrument Group has translated the severity provided by the vendor into labels that are more understandable by the group. The importance coding of the notification is determined by the Instrument Group based on other criteria, such as the availability of a backup meter on the same service. The designated recipient, Metrologist, is a member of the Instrument Group.

When the selected events occur for a specific instrument, the notification system automatically generates the alerts in the format selected by the recipient group. Instrument identification data are added. In this example, the following format is used:

Timestamp | *NotificationType* | *Importance* | *Instrument_Tag* | *InstrumentType* | *Nature of Event* | *Description*

The metrologist may receive the following notification:

The metrologist may receive the following notification

25-JUL-2019 00:07:05 ALERT 27FT1001 CORIOLIS FAILURE SLUG FLOW

Where,

- Notification type: ALERT
- Importance level: 1
- Location: Area 27
- Instrument tag: FT1001
- Instrument type: Coriolis
- Nature of Event: Failure
- Description text: Slug flow

Table 7 – Coriolis flow example

Event Description	Vendor Severity Code	Preferred Label	Instrument Type	Text	Notification Type	Importance no Backup	Importance with Backup	Recipient
Gas bubble in liquid (slug flow)	S	Failure	CORIOLIS	SLUG FLOW	Alert	1	2	Meter-ologist
Fouling, clogging	S	Degraded	CORIOLIS	FOULING	Alert	2	3	Meter-ologist
Erosion, corrosion	S	Incipient	CORIOLIS	CORROSION	Alert	3	4	Meter-ologist
Faulty mounting	M	Incipient	CORIOLIS	FAULTY MOUNTING	Alert	4	7	Meter-ologist
Asymmetry of measuring tubes (dual tube only), e.g. plugging	S	Degraded	CORIOLIS	TUBE PROBLEM	Alert	3	4	Meter-ologist
External vibrations	M	Incipient	CORIOLIS	EXTERNAL VIBRATIONS	Alert	4	7	Meter-ologist
Pulsating flow	S	Degraded	CORIOLIS	PULSATING FLOW	Alert	2	3	Meter-ologist
Incomplete filling	S	Degraded	CORIOLIS	EMPTY PIPE	Alert	2	3	Meter-ologist

Key

Vendor Severity Code

(S) Out of specification

(M) Maintenance request

(F) Failure

(C) Functional check

11.3 Equipment group – predictive failure diagnostic

As part of a new project, a compressor controller is installed. The vendor claims it has the ability to predict sub-component failure well in advance. The project's engineering equipment group is interested in how well the controller works over time, as other projects may use similar devices if proven effective.

The possible events that may be generated from the controller are prediction of sub-component failures, no sooner than 8 weeks in the future. The equipment group decides that the prediction events should produce the following notifications:

- Alarm: An alarm is not needed as there is no timely operator action to take.
- Alert: An alert should be generated to the site's equipment reliability group. Their responsibility and action are to confirm the likely validity of the diagnostic. If true, they are then responsible for coordinating with Operations and Maintenance to schedule and accomplish the fix, while minimizing the production impact.
- Notice: An informative notice that the predictive function has triggered should be generated to the original engineering equipment group. The group has no urgent action to take, but intends to now review the performance and diagnostic logs, checking the algorithms and machine reasoning that resulted in the prediction. Once the likely-to-fail component is removed, they will be interested in determining whether the prediction was accurate, and whether similar devices should be purchased on other projects.

Since it may take more than a year for any sub-components to fail, the alert message needs to include the following information:

- Time stamp
- Equipment identifier (compressor number and location)
- Event source (Predictive Program)
- Importance to the Equipment Reliability Group
- Sub-component name
- Descriptive message text (“Possible Failure Predicted”)

11.4 Pipeline pump maintenance group – pump seal failure prevention

High vibrations on a pump can lead to a pump trip and a line shutdown. In pipeline operation, vibration is not always caused by mechanical failure; a production change can create a high vibration. Currently, to reduce unnecessary callouts to the field, the Operator can reset the vibration alarm, adjust process parameters (such as pressure and flow to reduce the load on the pump), and continue to operate the line as per procedures. If the alarm occurs again within 15 minutes the line will shut down and lock out the line. The field will then be called to check the vibration and reset the line lockout. If the repeat vibration alarm does not occur again within the 15 minutes, the field will not be notified.

The high vibration maybe an indication that the pumps or seals are failing. Since the alarm reset, the Operator will not call the field or enter a Maximo (maintenance ticket) and the field will be unaware that there was a vibration issue. The next time there is a vibration alarm, the pump or seal may fail. If the redundant pump is out for maintenance this could become a major issue whereas if the field knew about the first vibration, they may have expediated the repair on the redundant pump or identified an issue with the operator pump and put operational restriction on it.

The pump maintenance group may decide to issue a prompt to the field at the same time as when the first high vibration alarm is issued to the Operator. The Field Operator can check the pump when on that site completing normal day-to-day activities. If it is operating outside normal parameters a Maximo would be generated to resolve the issue.

Field Operator training should include how to receive and respond to the notifications.

The notifications should include the following information at a minimum:

- Time stamp
- Pump identifier/location
- Descriptive message (“Check for high vibration”)
- Vibration measurement when alarm occurred

Bibliography

ANSI/ISA 18.2-2016 Management of Alarm Systems for the Process Industries

ISA-TR18.2.4-2012 *Enhanced and Advanced Alarm Methods,* ISBN 978-1-937560-19-5

ISA-TR18.2.6-2012 *Alarm Systems for Batch and Discrete Processes*, ISBN 978-1-937560-18-8

ANSI/ISA–88.00.02–2001 *Batch Control Part 2: Data Structures and Guidelines for Languages*

ISA–TR88.00.02 *Machine and Unit States: An Implementation Example of ISA-88*

ISA-TR-88.95.01 *Using ISA-88 and ISA-95 Together* ISBN: 978-1-934394-78-6

ANSI/ISA-95.00.06-2014 *Enterprise-Control System Integration-Part 6: Messaging Service Model*

ISO 10241-1:2011 *Terminological entries in standards*

IEC 62682 Edition 1.0 2015-10 *Management of alarm systems for the process industries*

EEMUA Publication 191 Edition 3 2013 *Alarm systems – Guide to design, management and procurement* ISBN 978-0-85931-192-2 (page 13)

ANSI/ISA-101.01-2015 *Human Machine Interfaces for Process Automation Systems* ISBN: 978-1-941546-46-8