Alarm Rationalization and Implementation

LISTEN.
THINK.
SOLVE.®

Allen-Bradley • Rockwell Software

Rockwell Automation

Introduction

The purpose of this white paper is to define the scope of the Alarm Rationalization and Implementation phases and how they continue the process of meeting the ANSI/ISA 18.2 Standard: Management of Alarm Systems for the Process Industries. It also addresses the third entry point into the standard: Audit.

Alarm Rationalization is the process of reviewing, validating, and justifying alarms that meet the criteria of an alarm. In other words, the rationalization specifies only those points in the process system that require alarming. The ultimate goal of Alarm Rationalization is to determine the most efficient number of alarms to ensure that the process system is safe and remains within the normal operating range.

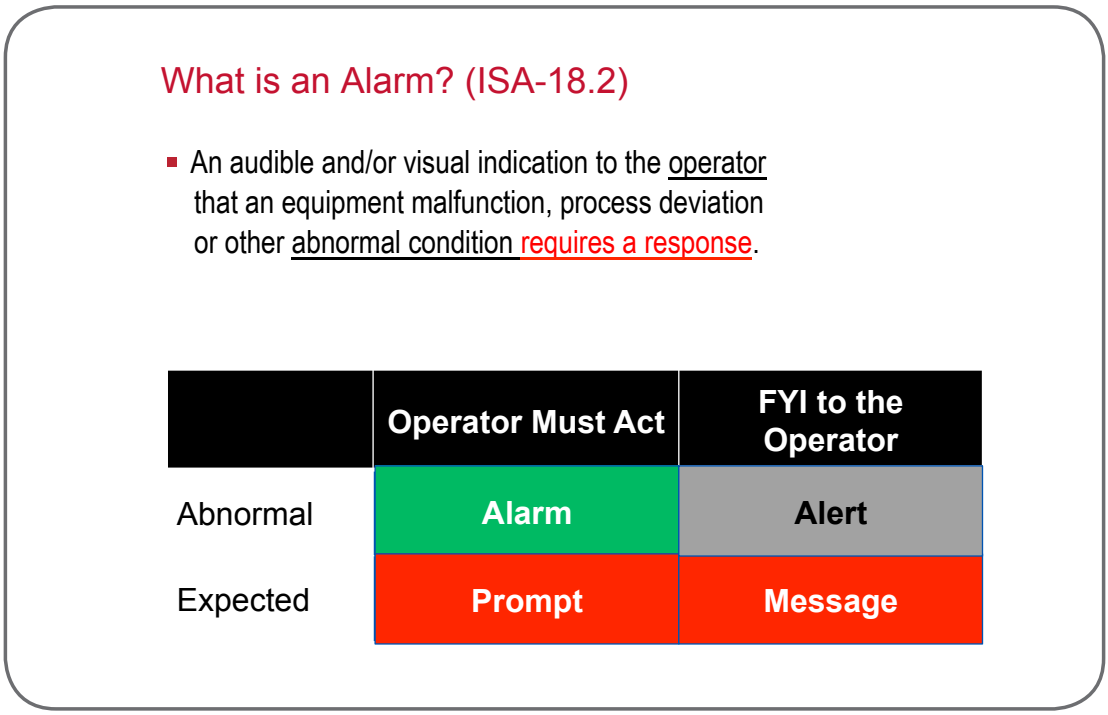


Figure 1

Implementation is the stage when alarms are put into operation. During this stage training, testing and commissioning occur. Finally, the Audit entry point into 18.2, which should be used periodically, is for verifying alarm system integrity.

This whitepaper is the third in a series of whitepapers that address the 18.2 lifecycle stages:

1. **Monitoring & Assessment** – A limited, but effective, program of nuisance/bad actor alarm elimination.

2. **Performance Benchmarking and Philosophy** – Benchmarking includes alarm analysis, operator analysis, and gap analysis. The Philosophy stage results in a document that details the recommended approach to how a company addresses alarm management through all stages of the lifecycle.

3. **Rationalization and Implementation** – Rationalization is the process of reviewing and justifying alarms that meet criteria that are established in the Philosophy Document. Implementation includes all of the infrastructure changes to support a new alarm system or modifications to an existing alarm system.

The first white paper illustrates how Monitoring & Assessment is an economical and manageable first step for identifying and eliminating nuisance/bad actor alarms. These alarms can account for as much as 80% of a system's alarm load. Monitoring & Assessment as a first step provides credibility and inertia toward implementing a more comprehensive alarm management program as resources and time permit.

The Benchmarking and Alarm Philosophy Development stages of 18.2, addressed in the second white paper, continue the process toward achieving comprehensive alarm management as recommended in this three-part series. Benchmarking builds upon the Monitoring & Assessment entry point and provides an initial performance baseline for ongoing comparison. The Alarm Philosophy Document includes requirements for effective design, implementation, and management of an alarm system – whether modifying an existing alarm system or implementing a new one.

Following the Rationalization steps outlined in this white paper results in an examination of every alarm in an existing system, providing an opportunity to correct configurations as necessary, improving system performance. For new systems, Rationalization helps determine initial alarm configuration. The Implementation phase includes the actual steps for installation of the new alarm system configuration, making it a reality and ensuring proper operational status.

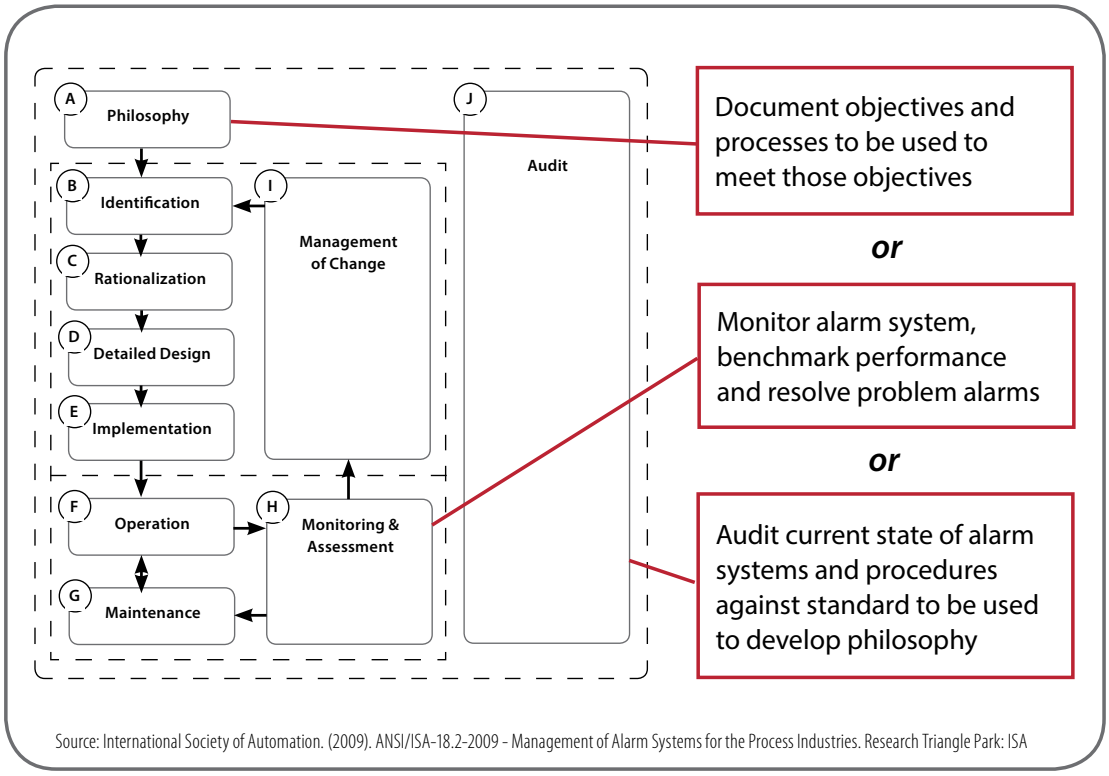
Overview of ANSI/ISA 18.2 Lifecycle

The ANSI/ISA 18.2 standard was developed to help the process industries design, implement, operate, and maintain effective alarm management systems.

Figure 2 illustrates the 18.2 lifecycle. It provides workflow processes and common alarm management terminology.

In all process industries, safety is paramount. Because a faulty alarm system can contribute to process accidents, using the 18.2 standard helps improve safety and incident prevention, reduce unplanned downtime, and improve regulatory and best practices compliance.

The 18.2 standard was developed to help engineering and technical staff identify ways to improve alarm management systems. It does not include information about how to implement and/or improve these systems in the most effective and economic manner.



Source: International Society of Automation. (2009). ANSI/ISA-18.2-2009 - Management of Alarm Systems for the Process Industries. Research Triangle Park: ISA

Figure 2

Figure 2 illustrates the 18.2 alarm management lifecycle, including three entry points. For new alarm system projects, the starting point is always the Philosophy stage. For existing systems, however, it is expedient, effective, and economical to begin with Monitoring & Assessment. The Audit is the third entry point.

The Alarm Rationalization Process

Establishing the minimum set of alarms necessary to keep a process safe and in normal operating condition is the goal of an Alarm Rationalization. The Rationalization process validates potential alarms by assessing them in terms of the alarm criteria defined in the Alarm Philosophy Document. The Alarm Rationalization process consists of the following steps:

1. Check Alarm Validity
2. Determine Consequence of Inaction
3. Document Cause, Confirmation, and Corrective Action
4. Document Operator Response Time
5. Assign Alarm Priority
6. Alarm Classification
7. Determine Alarm Limit
8. Verify/Establish Alarm Attributes
9. Assess Need for Special Handling

Steps 1 – 4 constitute the "knock-out" criteria for identifying non-alarms.

Process alarm systems are intended to provide operational awareness and assist operators in the diagnosis and remedy of abnormal conditions, reducing incidents and accidents. As noted in these white papers, poorly implemented alarm systems can, however, have the opposite affect by overloading operators with too much information, causing confusion and masking core problems in need of attention. That is why the major goal of the Alarm Rationalization is to determine the optimum number of alarms to assist operators, while ensuring safety and normal process operations.

Proper Alarm Rationalization requires a significant effort. There are two approaches to a Rationalization depending on the state of the alarm system.

The first approach is for existing process systems and should occur after the Monitoring & Assessment entry point and Benchmarking stages are complete. With this approach, the baseline is an existing alarm system configuration. During the Rationalization, decisions will be made whether to keep alarms as they are, modify configuration parameters as necessary, or eliminate unnecessary alarms. In some cases, new alarms may also be specified during this process. The focus for this white paper is on existing alarm systems.

The second approach is used when implementing an entirely new alarm system. Conducting a Rationalization for a new system is based on input from the Philosophy Document, which states alarm management objectives, as addressed in the second white paper in this series.

Alarm system consultants and technicians can be called upon to assist a facility's internal team with the Alarm Rationalization. They have the experience and knowledge to address problems associated with each step of the Rationalization and the expertise to provide the best solutions for each challenge.

The Alarm Rationalization team typically consists of both full- and part-time resources. ISA TR 18.02 (draft) states that the team can consist of the following from each category.

Full Time:

- Production and/or process engineers familiar with the process, economics, and the control system
- Operators from different shift teams with experience in the use of the control system
- Process control/industrial engineer
- Alarm management consultant/analyzer specialist

Part Time:

- Safety and environmental engineer
- Maintenance/equipment reliability
- Instrumentation/analyzer specialist
- Management sponsor

Optimum team size is four to five people, according to Exida.

Selecting Alarms for Rationalization – Identify Potential Alarms and Determine if they are Valid for Specification

When a potential alarm is selected for consideration, it must first be evaluated against the "knock-out" criteria (validity, consequence of inaction, corrective action, and response time). Assuming that the alarm survives this evaluation, the next steps include defining the attributes of the alarm – priority, classification, and limit – where all of this information is used to build the Master Alarm Database.

See Figure 3 for an overview of the Rationalization steps addressed in this white paper.

Alarms Validity

A common alarm validity checklist includes these types of questions:

1. Does the alarm indicate a deviation or processing malfunction that requires operator action?
2. What is the importance of the condition? What are the consequences of no operator action?
3. Does it provide time for the operator to act effectively and in a timely manner to avoid possible consequences?
4. Is the alarm unique and does it capture the root cause of the malfunction or abnormality?

If these criteria are not met, then the condition does not require an alarm and the rationale for the decision should be documented.

The Alarm Rationalization Process

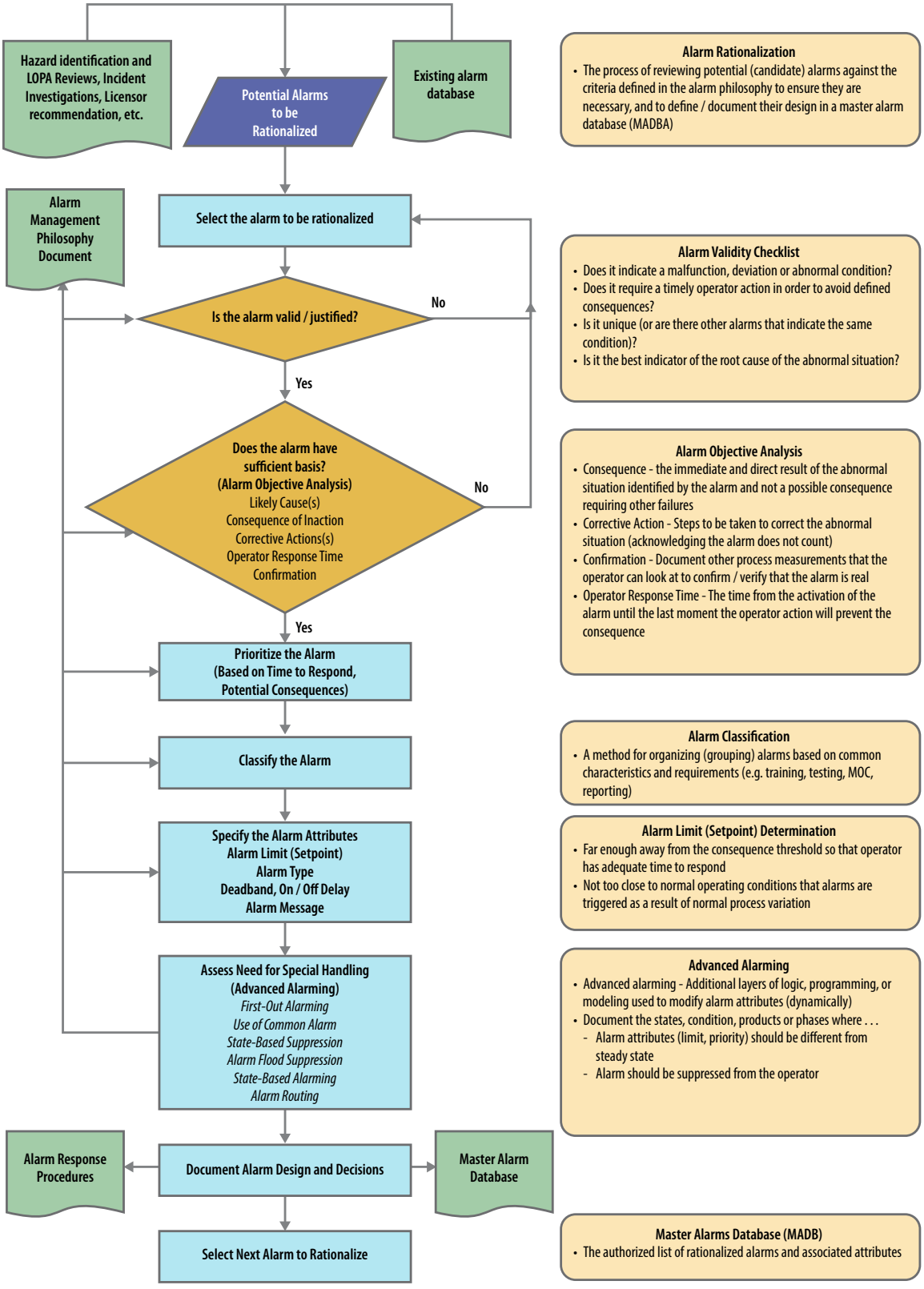


Figure 3

Consequence of Inaction

In order to be an alarm, the condition should indicate an abnormal situation that has an immediate and direct consequence if no action is taken. The consequence should not be dependent on additional failures. If there is no consequence, than the condition does not warrant an alarm.

Cause, Confirmation, Corrective Action

For a justifiable and valid alarm, document the following attributes:

1. **Cause** – List of likely events, expected or unexpected, that this alarm uniquely identifies.
2. **Confirmation** – Other process measurements/conditions that will help the operator establish that the alarm is real and identify which likely event caused the alarm.
3. **Corrective Action** – Objective actions the operator will take to correct the abnormal situation. Simply acknowledging the alarm is not an action. If there is no corrective action stated, the condition does not warrant an alarm.

Alarm Definition – Frequently Asked Question

Q: When is it OK to have both a High and High-High alarm for a single tag?

A: When either alarm has different Cause or Consequence or Operator Action.

Operator Response Time

Operator response time is defined as the time from the activation of the alarm to the moment at which the operator's corrective action prevents the consequence. When the operator response time available is less then that needed to adequately confirm the alarm and take corrective action, it is necessary to automate the response (i.e., interlock) rather than create an alarm.

The steps above constitute the "knock-out" criteria that help to identify and eliminate those conditions not warranting an alarm. For conditions that have survived, rationalization continues with the following steps.

Prioritizing Alarms

This step determines the importance assigned to an alarm within the alarm system based on operator response time and potential consequences. Prioritization specifies how the operator manages operational risk; that is:

- The severity of the consequences resulting from inaction
- The time available to take corrective action

Alarm Prioritization Methodology

Consequences of Inaction				
Impact Areas	**Consequence Category 1 (None)**	**Consequence Category 2 (Minor)**	**Consequence Category 3 (Major)**	**Consequence Category 4 (Severe)**
Personnel	None	Minor or no injury, no lost time.	One or more severe injury(s).	Fatality or permanently disabling injury.
Environmental	None	Minor	Release which results in agency notification, permit violation or fine.	Significant release with serious offsite impact.
Financial	None	Impact to equipment or production < $50K.	Impact to equipment or production $50K to $500K	Impact to equipment or production > $500K
Operator Urgency (Time to Respond)				
Not Urgent (> 30 mins)	**No Alarm**	**Re-engineer the alarm for urgency**		
Prompt (15 to 30 mins)	**No Alarm**	**Medium**	**Medium**	**High**
Rapid (5 to 15 mins)	**No Alarm**	**Medium**	**High**	**Highest**
Immediate (< 5 mins)	**No Alarm**	**High**	**Highest**	**Invalid (redesign)**

Figure 4

Referring to Figure 4 – Alarm Prioritization Methodology, "Consequences of Inaction" provides a consequence impact grid and "Operator Urgency" information that includes attributes used to help the operator determine the order in which alarms should be addressed.

In the "Consequences of Inaction" grid, each impact category should be considered separately and it must be completely understood how minor or severe consequences will be in each category – in this case three: personnel, environmental, and financial – if no operator action is taken in response to an alarm or alarms. This grid is one of the cornerstone elements of the rationalization process. It includes descriptions of consequences that must be clear and objective, ensuring that different people evaluating the same event/occurrence agree with the assessment of severity.

When designing an "Operator Urgency" grid, it is recommended to use no more than three or four priority levels. The example in Figure 4 uses thee: high, medium and low. These levels are established from data based on the severity of the consequences and the operator's specified time to respond, from immediate to not urgent.

Alarm response procedures should be put into place to help operators respond more effectively to an alarm. Documented procedures should identify likely causes(s) for the alarm, consequences of operator inaction, appropriate operator actions, confirmation that the alarm is not false, and the amount of time for the operator to successfully respond to the alarm.

Alarm Classification

The purpose of this activity is to identify groups of alarms that have similar characteristics and common requirements. There are no identified or required instances of alarm classifications in the ISA 18.2 standard. It is recommended to keep classification simple, such as these suggested groups with the following alarm characteristics:

- Environmental
- Process Safety
- Building/Facility Related
- Diagnostics
- Devices External to the Control System

Other methodologies for determining alarm classification include:

- Method of identification – Alarms identified in a Layer of Protection Analysis are assigned to LOPA Listed Class.
- Consequences – Alarms are assigned to classes according to their potential to do harm.
- Company Policy – Alarms are assigned to classes created to align with company policy.

It should be recognized that alarms can be members of more than one class, and that not all alarms in a class need to have the same priority.

Alarm Limit (Setpoint) Selection – Because manufacturing processes are dynamic, variables such as alarm limits may change over time. The key to establishing alarm limits is to set the alarm activation point far enough away from the potential consequence to ensure the operator has enough time to respond to the alarm. In addition, it is also important to set the limit such that it is not is too close to normal process operating conditions to prevent the alarm from being triggered during normal process variations.

Statistical analysis of process history can prove to be a useful too for determining normal operating ranges and optimum alarm limit selection.

Establish/Verify Alarm Attributes (Optional)

An optional yet valuable step in the Alarm Rationalization process is to establish/verify alarm attributes, including:

- Alarm Type
- Alarm Deadband (Hysteresis)
- Alarm On-Delay
- Alarm Off-Delay
- Process Variable Filter
- Alarm Latching

While these parameters may be considered during design, it is often convenient and appropriate to revisit them during Rationalization to ensure that the alarm system performs as designed/expected.

Advanced Alarming Considerations

Advanced alarming includes additional layers of logic and programming to address alarm situations that are beyond steady state process control. For example, process equipment usually has several different operating states (e.g., starting, running, continuous operation, shutdown, etc.) and advanced alarming techniques can be used to modify the associated alarm attributes. In these cases, it is necessary to document different states, conditions, and products or phases where alarm attributes should be different, or perhaps, suppressed from the operator.

Advanced alarming methods include alarm suppression, alarm shelving and alarm disabling. State-based suppression is used to suppress alarms that are not meaningful when a process area, unit or piece of equipment is in a particular operating state (mode):

- Designed Suppression: Suppresses alarms based on operating conditions or plant states – under control of logic that determines the relevance of the alarm.
- Shelved: A mechanism, typically initiated by the operator, to temporarily suppress an alarm.
- Out of Service: The state of an alarm during which the alarm indication is suppressed, typically manually, for reasons such as maintenance.

Documentation and the Master Alarm Database

The Master Alarm Database (MADB) is the authorized list of rationalized alarms and their associated attributes. It serves as the required documentation from Rationalization with alarm instance data such as:

- Alarm Type
- Alarm Priority
- Alarm Class
- Alarm Limit (Setpoint)
- Operator Action
- Consequence of Inaction
- Need for Advanced Alarming Techniques

When preparing the MADB for an existing system, software tools such as the PlantPAx® Alarm Builder from Rockwell Automation and SilAlarm from Exida, can be used in conjunction to facilitate data exchange between the DCS and the Master Alarm Database.

Alarm System Implementation

Implementation is the stage where alarms are put into operation. This stage also includes plant infrastructure changes to support the updated or new alarm system. As with any DCS project, good engineering practices will lead to a successful Implementation.

At the completion of the Alarm Rationalization, and when alarm system enhancements and redesigns are complete, it is time to proceed to Implementation. Much more than changing alarm parameters and eliminating unnecessary alarms, the Implementation stage includes training, testing and commissioning.

With the appropriate software tools, all of the updated design code for the system is prepared for downloading into the DCS. Plant infrastructure changes are implemented as well. Examples to tools that support the new alarm system include graphics, procedures, and HMI to name a few. Training materials must be prepared and reviewed; all plant-related documentation needs to be updated. Operators and other appropriate personnel are trained to manage the new alarm system. Some plants have simulators and can test the system and train operators at the same time.

The new configurations are downloaded and activated. This includes replacing old procedures and guidelines with the new ones, activating all remaining changes, and reviewing all downloads to ensure correct operation. It is now time to prepare for the final cutover to the new alarm system.

Periodic Alarm System Audits

Periodic audits, verifying alarm system integrity, are recommended to review overall alarm management processes. The Alarm Philosophy Document and the Master Alarm Database are used as the starting points for the Audit. Figure 5: Audit Differences Between DCS and Master Alarm Database shows a sample Differences Report.

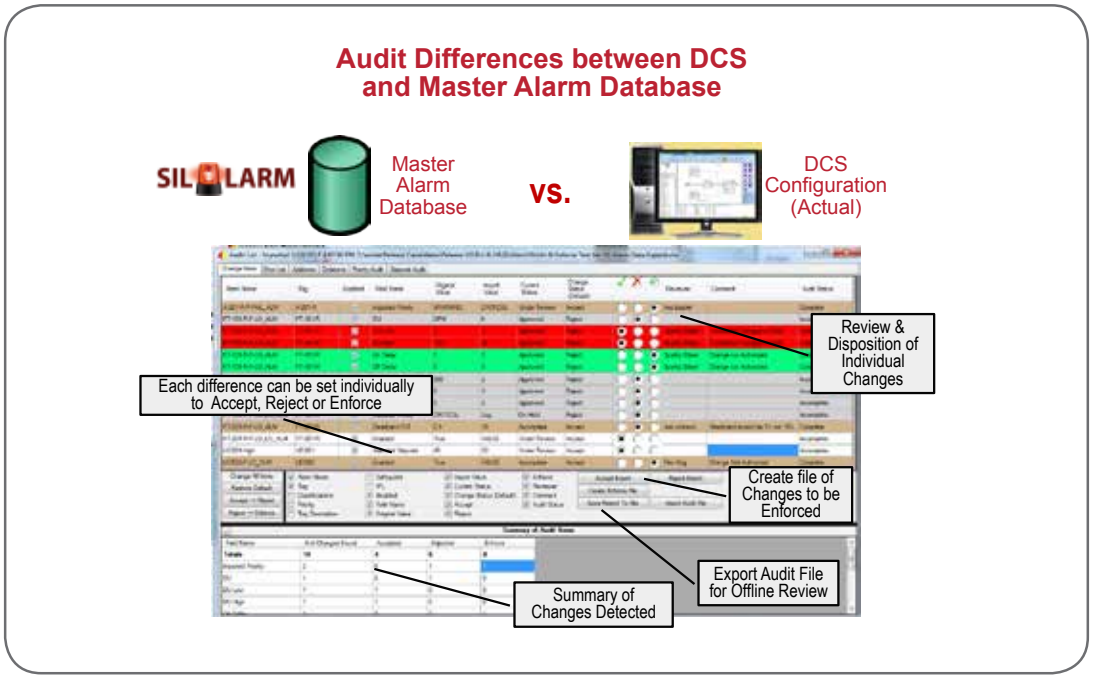


Figure 5

The Audit, which is the third entry point into the ISA 18.2 lifecycle, is important because it identifies areas of improvement for any and all of the stages of the lifecycle, including Philosophy Development, Identification and Benchmarking, Rationalization, Monitoring & Assessment, Operation, Maintenance and Management of Change.

Benefits of 18.2 Alarm Rationalization and Implementation

Proper alarm management is an ongoing commitment. As noted in the first white paper, the Monitoring & Assessment entry point delivers immediate early success, but shouldn't be the sole step for improving the alarm system. The second white paper addresses how Benchmarking and Alarm Philosophy Development provide the next steps toward a comprehensive alarm management system.

Completing the Rationalization and Implementation stages of the 18.2 lifecycle result in an updated, effective alarm management system that fulfills the goal of ISA 18.2 compliance. Taken together, each stage of the 18.2 lifecycle results in three primary benefits: improved productivity, increased plant safety, and improved regulatory compliance.

Improved Productivity – Poor alarm system performance negatively affects operators and operations. It's one of the leading causes of unplanned downtime. Operators waste time dealing with the confusion caused by too many alarms and the unreliable information from nuisance alarms. Effective alarm management helps eliminate waste, improve processing quality, and increase productivity.

Increased Plant Safety – Alarm flooding impairs plant safety because of possible confusion when dealing with multiple nuisance alarms in short periods of time. Operators are uncertain about which alarms require priority response. Proper alarms meant to prevent plant incidents become ineffective in a flood of alarms. The 18.2 standard helps provide a blueprint for effective alarm management and increased plant safety.

Improved Regulatory and Best Practices Compliance – Implementing an alarm system that complies with the ISA 18.2 standard helps ensure a comprehensive and effective alarm management program to support and assist process system operators with ANSI/ISA best practices.

See the first two white papers in this series for information about Monitoring & Assessment, Benchmarking, and Philosophy Development.

References

Holifield, Bill and Habibi, Eddie: *The Alarm Management Handbook,* Second Edition: A Comprehensive Guide; August 31, 2010

Rothenberg, Douglas: Alarm Management for Process Control: Momentum Press, 2009

Abnormal Situation Management – ASM Consortium: *Effective Alarm Management Practices 2009*

Grosdidier, Pierre (Ph.D., P.E.); Conner, Patrick (P.E.); Hollifield, Bill; Kulkarni, Sarmir: *A Path Forward for DCS Alarm Management;* published by Plant Automation Services, Inc.

Van Camp, Kim (Emerson Process Management) and Stauffer, Todd (PE, exida): *Tips for Starting an Alarm Management Program;* published in Applied Automation; April 2013

Exidia – The ISA 18.2 Alarm Management Lifecycle

Exida – Alarm Management is a Journey

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication PROCES-WP015B-EN-P – June 2017
Supersedes Publication PROCES-WP015A-EN-P – April 2015