ALARM MANAGEMENT GUIDELINE

EGPC-PSM-GL-019

PSM GUIDELINES

The Egyptian Process Safety Management Steering Committee (PSMSC Egypt)
PSM TECHNICAL SUBCOMMITTEE (PSMTC)

Acknowledgments

This publication has been produced as a result of the comprehensive efforts carried out by the PSM Technical Subcommittee on behalf of the Egypt PSM Steering Committee, formed per the Memorandum of Understanding signed between the Ministry of Petroleum and Mineral Resources and Methanex Egypt in February 2020 overseeing the design and implementation of a detailed PSM program to promote and enhance PSM culture for Ministry of Petroleum and Mineral Resources (MOP) and its affiliated COMPANIES following industry best practice, international codes, and standards. The Egyptian Process Safety Management Steering Committee comprises MOP, EGPC, ECHEM, EGAS, GANOPE, and Methanex Egypt representatives.

PSM Technical Subcommittee team members during the project comprised:

Amr Moawad Hassan	**PSM Senior Consultant – Methanex Egypt**	**Team Leader**
Sayed Eid	HSE A. General Manager – Agiba Pet. Co.	Member
Ahmed Mostafa	Operations Section Head - ELAB	Member
Ahmed Roustom	Risk Management and Loss Prevention Studies Assistant General Manager – GASCO	Member
Hany Tawfik	OHS & PS General Manager – ETHYDCO	Member
Mohamed Ashraf Aboul-Dahb	Safety Section Head for Upstream – EGPC	Member
Mohamed Mesbah	Operations Department Head - KPC	Member
Mohamed Hamouda	HSE Department Head – Pharaonic Pet. Co.	Member
Mohammed Sabry	Risk Management and Loss Prevention Studies Executive General Manager – GASCO	Member
Tamer Abdel Fatah	QHSE Senior – UGDC	Member

All PSM technical subcommittee documents are subjected to a thorough technical peer-review process during development and prior approval. The PSM technical subcommittee gratefully appreciates the thoughtful comments and suggestions of the peer reviewers. Their contributions enhanced the accuracy and clarity of the documents. The PSM Technical Subcommittee acknowledges the following reviewers from major Process Safety consultants as well as major operators & EPC contractors who provided valuable comments during the technical peer reviews that resulted in an outstanding product structure and quality:

Process Safety Consultants (in alphabetical order):

- Ahmed Ismail, Operations department Head (Badr Eldin Petroleum Company).
- Aladdin Elsonbati, HSE & Process Safety Manager (ENI).
- Exida - By: Greg Chantler, Principal Consultant.

It should be noted that the above have not all been directly involved in developing this document, nor do they necessarily fully endorse its content.

Egypt PSM Steering Committee team members during the project comprised:

Gamal Fathy	EGPC CEO Consultant for HSE – EGPC	Member
Mohamed Mahmoud Zaki	Executive Vice President – ECHEM	Member
Salah El Din Riad	Q&HSE Chairman Assistance – ECHEM	Member
Dr. Ashraf Ramadan	Assistant Chairman for HSE – EGAS	Member
Emad Kilany	OHS & Fire Fighting Technical Studies GM - EGAS	Member
Mohamed Sayed Suliman	HSE General Manager – GANOPE	Member
Mohamed Mostafa	Inspection & External Audit GM – ECHEM	Member
Mohamed Shindy	Managing Director – Methanex Egypt	Member
Manal El Jesri	Public Affairs Manager – Methanex Egypt	Member
Mohamed Hanno	RC Manager – Methanex Egypt	Member
Amr Moawad Hassan	PSM Senior Consultant – Methanex Egypt	Member
Mourad Hassan	PSM Consultant – Methanex Egypt	Member

DOCUMENT NO.	TITLE	ISSUE DATE
EGPC-PSM-GL-019	ALARM MANAGEMENT GUIDELINE	DEC. 2022

Approval

NAME	TITLE	DATE	SIGNATURE
Amr Moawad Hassan	PSM Senior Consultant - Methanex Egypt PSM Technical Subcommittee TL	DEC. 2022	Amr Hassan Digitally signed by Amr Hassan Date: 2022.12.29 09:03:40 -06'00'
Gamal Fathy	EGPC CEO Consultant for HSE	DEC. 2022	Gamal Fathy

Endorsement

NAME	TITLE	DATE	SIGNATURE
Alaa El Batal	CEO - Egyptian General Petroleum Corporation (EGPC)	DEC. 2022	

Controlled Intranet Copy

The intranet copy of this document is the only controlled document. Copies or extracts of this document, downloaded from the intranet, are uncontrolled copies and cannot be guaranteed to be the latest version. All printed paper copies should be treated as uncontrolled copies of this document.

All administrative queries must be directed to the Egyptian Process Safety Technical Subcommittee.

Table of Contents

1. Introduction

It is important to start the introduction with the statement of Lucius Annaeus Seneca "There are more things to alarm us than to harm us, and we suffer more often in apprehension than reality." This statement puts the base of the alarm system, which is how it anticipates the undesired events or situations and draws people's attention to this before it gets worse and the real loss occurs.

The alarm system's main purpose is to notify the operator about the presence of abnormal events, conditions, or malfunctions of any part of plant equipment and support the response. In other words, the alarm system can be considered the backbone for ensuring the safe operation of the plant and meeting the production targets.

The alarm system is one of the layers of protection or one of the risk reduction measures for the safety of the plant and to prevent or relieve the escalation of any abnormal or undesired event, as illustrated in Figure 1.

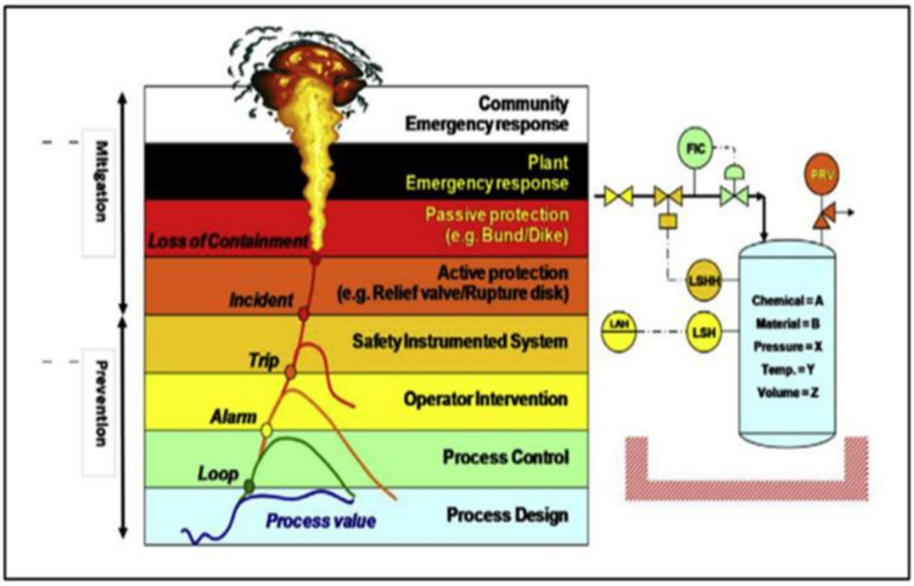


Figure 1. *Layers of protection.*

Looking at the different layers of protection and their ordering, it is clear that a properly functioning alarm system and timely operator response will prevent escalation of the emergency scenario and end the emergency. But what happens if the alarm system and the operator intervention are delayed or fail to function? The emergency becomes more complex. A further escalation occurs with the potential for plant shutdown and production losses. Finally, it might lead to loss of containment with the potential of multiple fatalities/injuries and impact on the environment and surrounding community.

The alarm systems can include the basic process control system (BPCS) and the safety instrumented system (SIS), each of which uses process conditions and logic measurements to generate alarms. Figure 2 illustrates the concepts of alarm and response dataflow through the alarm system. The alarm system also includes a mechanism for communicating the alarm information to the operator via Human-Machine Interface (HMI), usually a computer screen or an annunciator panel. Additional functions of the alarm system are an alarm and event log, an alarm historian, and the generation of performance metrics for the alarm system.

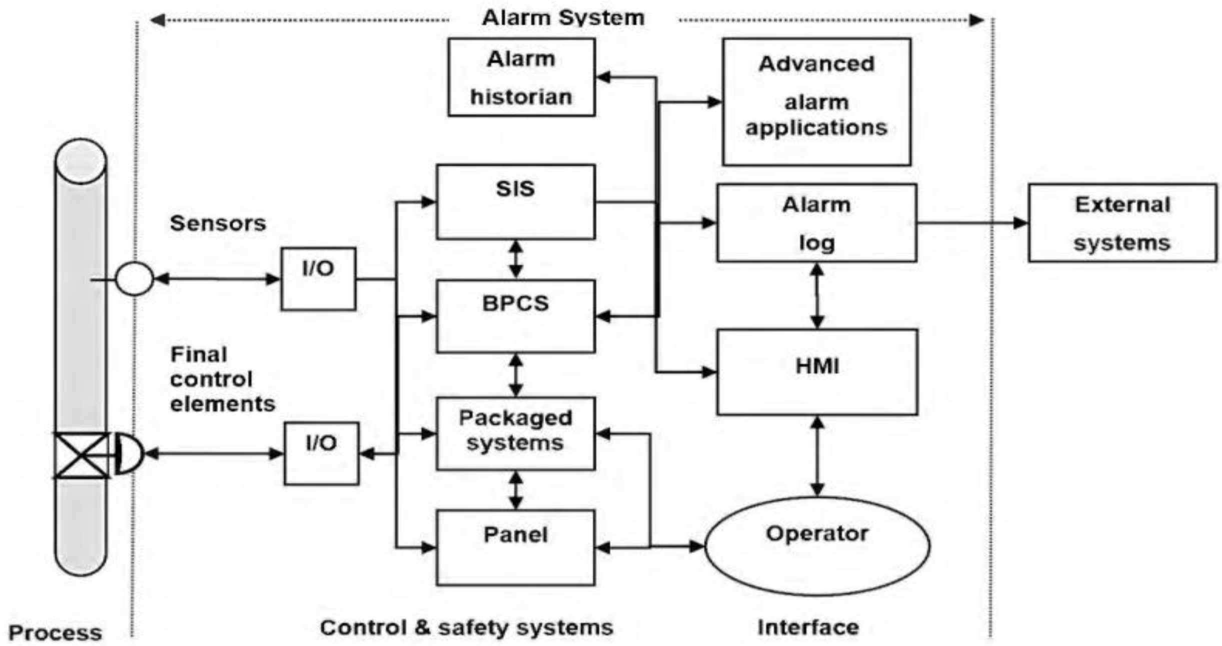


***Figure 2**. Alarm system dataflow.*

The industry history, especially in oil and gas, has a big record of accidents where the poor alarm management system was the cause of the accident. For example, the investigation of the Milford Haven refinery explosion in the 1994 report shows that the main causes of the incident were: the generation of too many alarms, poor prioritization, poor control room display, and alarm flooding, which reached 275 alarms per 11 minutes. Another example is BP Texas City 2005, where the major causes were the failure of key alarms to warn the operators about the unsafe conditions in the tower and the closure of the blowdown condition, which led to fire and explosion, 15 fatalities, and 180 injuries.

The current guideline discusses a collection of processes and practices that ensure an effective alarm management system with the consideration of human limitations.

2. Purpose

This guideline provides guidance on the principles and requirements for developing, operating, and maintaining an effective alarm management system. An effective alarm management system aims to enhance/improve the reliability and integrity of one of the critical layers of protection (Alarm and Operator Response) during a process fault or undesirable conditions.

3. Scope

The scope of this guideline includes an Alarm system for Greenfield, Brownfield, and Extensions/Modifications of an existing plant. This guideline applies to Egyptian General Petroleum Corporation (EGPC) and Oil & Gas Holding Companies, including the Egyptian Natural Gas Holding Company (EGAS), the Egyptian Petrochemicals Holding Company (ECHEM), and the South Valley Petroleum Holding Company (GANOPE) covering all their operational subsidiaries, state-owned companies, affiliates, and joint ventures.

4. Definitions

ACKNOWLEDGE: operator action that confirms recognition of an alarm.

ACTIVE ALARM: an alarm in a state in which the alarm condition is true.

ADAPTIVE ALARM: alarm for which the setpoint is changed by an algorithm (e.g., calculated based on production rate).

ADJUSTABLE ALARM: alarm for which the operator can change the setpoint manually.

ADVANCED ALARMING: a collection of techniques that can help manage annunciations during specific situations.

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

ALARM ANNUNCIATION: function of the alarm system to call the attention of the operator to an alarm.

ALARM ATTRIBUTE: setting for an alarm within the process control system, e.g., alarm priority.

ALARM CLASS: a group of alarms with a common set of alarm management requirements (e.g., testing, training, monitoring, and audit requirements). For example safety related alarms.

ALARM DEADBAND: change in signal from the alarm setpoint necessary for the alarm to return to normal.

ALARM FILTERING: function which selects alarm records to be displayed according to a given element or elements of the alarm record.

ALARM FLOOD: condition during which the alarming rate is greater than the operator can effectively manage (e.g., more than 10 alarms per 10 minutes).

ALARM GROUP: a set of alarms with a common association (e.g., process unit, process area, equipment set, or service).

ALARM HISTORIAN: a long-term repository for alarm records.

ALARM LOG: a short-term repository for alarm records.

ALARM MANAGEMENT: a collection of processes and practices for determining, documenting, designing, operating, monitoring, and maintaining alarm systems.

ALARM MESSAGE: text string displayed with the alarm indication that provides additional information to the operator (e.g., operator action).

ALARM OFF-DELAY: time an alarm remains active after the process measurement has returned within the alarm setpoint.

ALARM ON-DELAY: the time before an alarm becomes active after the process measurement has exceeded the alarm setpoint.

ALARM PHILOSOPHY: a document that establishes the basic definitions, principles, and processes to design, implement, and maintain an alarm system.

ALARM PRIORITY: relative importance assigned to an alarm within the alarm system to indicate the urgency of response (e.g., the seriousness of consequences and allowable response time).

ALARM RATE: number of annunciated alarms, per operator, in a specific time interval.

ALARM RECORD: a set of information that documents an alarm state change.

ALARM RESPONSE PROCEDURE: guidance for responding to an alarm (e.g., operator action, probable cause).

ALARM SETPOINT: threshold value of a process variable or discrete state used to determine if the alarm is active.

ALARM SYSTEM: a collection of hardware and software that detects an alarm state, communicates that state's indication to the operator, and records changes in the alarm state.

ALARM SYSTEM REQUIREMENTS SPECIFICATION: a document describing the alarm system's functionality.

ALARM TYPE: alarm attribute which gives a distinction of the alarm condition.

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

ALLOWABLE RESPONSE TIME: maximum time between the annunciation of the alarm and when the operator must take corrective action to avoid the consequence.

ANNUNCIATOR: device or group of devices that call attention to changes in process conditions.

CHATTERING ALARM: an alarm that repeatedly transitions between the alarm state and the normal state in a short period.

DEVIATION ALARM: alarm generated when the difference between two values exceeds an alarm setpoint (e.g., the deviation between primary and redundant instruments or between the process variable and controller setpoint).

DISCREPANCY ALARM: alarm generated by the difference between the expected plant or device state to its actual state (e.g., when a motor fails to start after it is commanded to the on the state).

FLEETING ALARM: an alarm that quickly transitions between the alarm state and the normal state without rapidly repeating.

HIGHLY MANAGED ALARM (HMA): alarm belonging to a class with additional requirements (e.g., regulatory requirements) above general alarms, e.g., safety alarms.

INSTRUMENT DIAGNOSTIC ALARM: alarm to indicate a field device or signal fault.

INTERIM ALARM: alarm used temporarily to replace an out-of-service alarm.

MASTER ALARM DATABASE: authorized list of rationalized alarms and associated attributes.

NUISANCE ALARM: an alarm that annunciates excessively, unnecessarily, or does not return to normal after the operator action is taken. For example, chattering alarm, fleeting alarm, or stale alarm.

SHELVE: temporarily suppress an alarm initiated by the operator with engineering controls (e.g., time-limited) that unsuppress the alarm.

STALE ALARM: an alarm that remains annunciated for an extended period (e.g., 24 hours).

5. Abbreviations

ASRS	Alarm System Requirements Specifications
BPCS	Basic Process Control System
EEMUA	Engineering Equipment and Materials Users Association
HMA	Highly Managed Alarm
HMI	Human-Machine Interface
PDCA	Plan, Do, Check, Act

For other definitions and abbreviations, refer to the PSM Glossary of Definitions and Abbreviations Guideline (EGPC-PSM-GL-011).

6. Alarm System

6.1 General

Alarm systems communicate indications of abnormal process conditions or equipment malfunctions to the operators, the personnel monitoring and operating the process, and support the response. Effective alarm systems are well-designed, implemented, operated, and maintained.

In concept, there are key principles identified for any alarm system:

- *Every alarm should have a defined purpose.* In general, the purpose of any alarm system is to drive the operator's attention to certain plant conditions that require a timely assessment and consequent actions. Thus, the alarm system will help the operator manage tasks and resources and focus on important issues. To achieve this, each alarm should alert, inform and guide the operator in the presence of certain circumstances. The operator should be easily notified when the alarm occurs through audible and visual aids. Moreover, the alarm should present information regarding the problem that occurred by descriptive messages, lighting a labeled announcer window, or changing the graphic display. The introduced information should also guide the operator in responding to the received alarm.
- *Every alarm should have a defined response.* Each alarm presented to the operator should be useful and relevant. To achieve this, the designer should ensure that every alarm has a defined response. This response should generally be an action, e.g., operating a standby pump, alerting a control set point, repairing some equipment failure part, etc. The signal should not be considered an alarm if the response cannot be defined. Finally, the way to present the required responses shall be defined by the designer and not mixed with alarms.
- *Adequate time should be allowed for the operator to carry out this response.* As discussed before, for each alarm, the operator response is expected. This requires that adequate time should be given for the operator to perform the required action. To achieve this, the alarm should occur early enough to allow the operator to correct the fault. Moreover, the alarming rate should not exceed the operator's capability for alarm handling per unit of time. Figure 3 represents a process measurement that increases from a normal to an abnormal condition and the two possible scenarios based on whether the operator takes the corrective action.

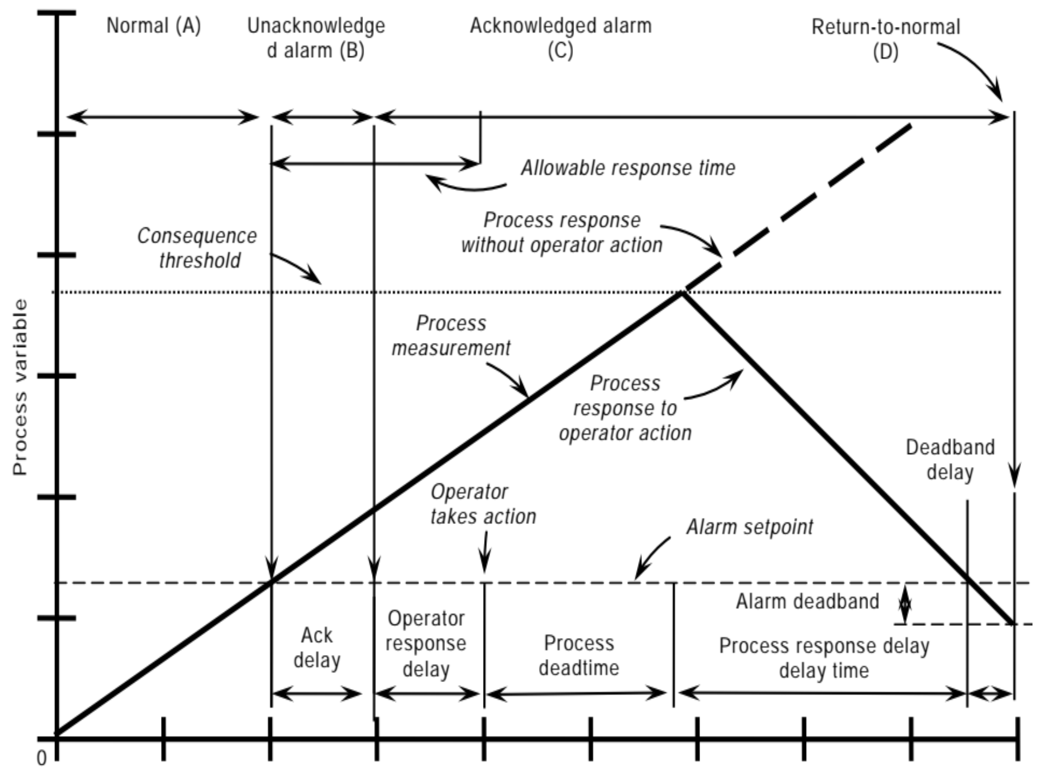


Figure 3. *Alarm response timeline.*

6.2 Criteria for Effective Alarm System

The alarm system should be designed to account for human limitations. Accordingly, an effective alarm system needs to include the following:

- *Any alarm should be Relevant:* this means that any alarm is not to be spurious or of low operational value. Looking at this alarm characteristic, it is important to mention that fall to develop a relevant alarm is the reason behind many incidents in the oil and gas industries.
- *Alarms should be Unique:* this means that each alarm should not duplicate another alarm.
- *The alarm should be Timely:* as mentioned before, the purpose of an alarm system is to direct the operator's attention to the presence of certain conditions requiring a timely assessment and actions. This characteristic of alarm means that the time of the alarm is not long before any required response or too late to perform the required response.
- *Alarm Prioritization:* this characteristic targets to indicate the importance that the operator deals with.
- *Understandable:* this characteristic ensures that each alarm message is clear and easily understandable by the operator(s).

- *Diagnostic*: this characteristic is about the system's ability to identify the problem(s) that has/have occurred easily. This is one of the core abilities of the system to detect and analyze the event and then deliver the right message to the operator to take suitable action on a timely basis.
- *Advisory:* this characteristic is about how the alarm system helps indicate the required action for each type of alarm.
- *Focusing:* this characteristic is very important with the general target to draw the operator's attention to the most important issues, not overloading with low-priority issues that can disturb the operator and affect its attention for a real case.

7. Alarm Management Lifecycle

Alarm management is a collection of processes and practices that ensure an effective alarm system. This can be achieved by ensuring well designed, implemented, operated, and maintained alarm system. The alarm management lifecycle covers alarm system specifications, design, implementation, operation, monitoring, maintenance, and change activities from initial conceptions. Like other management systems, it shall be managed by considering the PDCA cycle approach, i.e., the alarm management system will care for the alarm system starting from the specifications and proper design considering the operator's limitation and the nature of the plant. Then start the operation and testing/monitoring the system performance and purpose any required changes with the target of the whole system improvement.

This model aims to identify the requirements and responsibilities for implementing the alarm management system in a structured way. Figure 4 illustrates ISA 18.2 alarm management lifecycle model. This lifecycle model applies to installing and managing new and existing alarm systems.

The alarm management lifecycle stages are connected as the outputs of one stage are often the inputs of another. The lifecycle diagram does not fully represent the connections. Table 1 provides more information on the relationships between the inputs and outputs of the lifecycle stages.

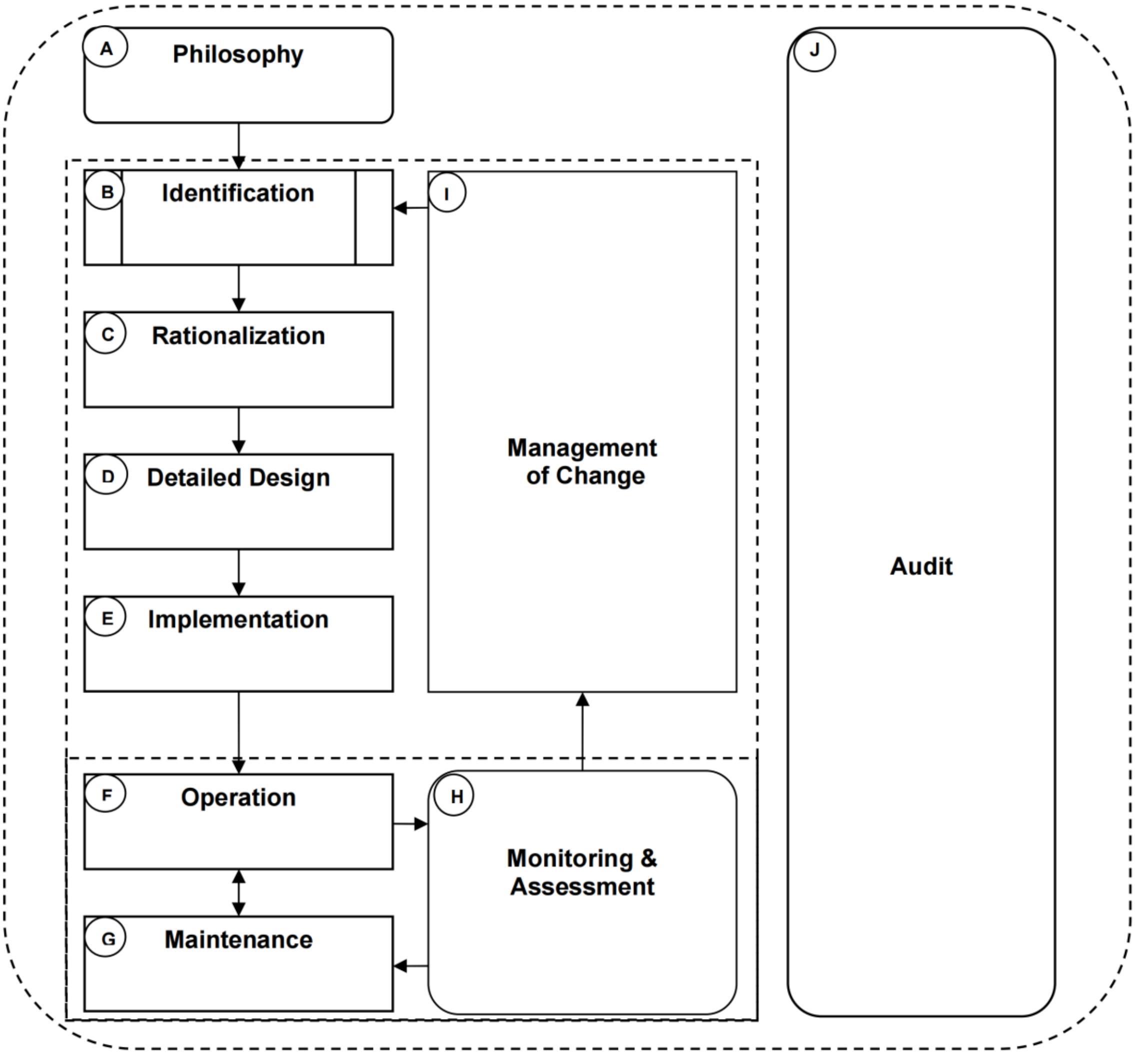


Figure 4. *Alarm management lifecycle [1].*

Table 1. *Alarm management lifecycle stage inputs and outputs.*

Alarm Management Lifecycle Stage		Activities	Inputs	Outputs
Stage	Title			
A	Philosophy	Document the objectives, guidelines, and work processes for the alarm system.	Objectives and standards.	Alarm philosophy and Alarm System Requirements Specification (ASRS).
B	Identification	Determine potential alarms.	PHA report, SRS, P&IDs, operating procedures, etc…	List of potential alarms.
C	Rationalization	Work process that determines which alarms are necessary, establishes their design settings (e.g., priority, limit, classification), and documents their basis (cause, consequence, corrective action, time to respond, etc) in a Master Alarm Database.	Alarm philosophy, and list of potential alarms.	Master alarm database, alarm design requirements.
D	Detailed Design	Designing the system to meet the requirements defined in rationalization and philosophy. Includes Basic alarm design, HMI design, and advanced alarming design.	Master alarm database, alarm design requirements.	Completed alarm design.
E	Implementation	Alarm system is put into operation (installation & commissioning, initial testing, and initial training).	Completed alarm design and master alarm database.	Operational alarms, Alarm response procedures.
F	Operation	Alarm system is functional. Operators use available tools (e.g., shelving and alarm response procedures) to diagnose and respond to alarms.	Operational alarms, alarm response procedures.	Alarm data.
G	Maintenance	Alarms are taken out of service for repair and replacement, periodic testing.	Alarm monitoring reports and alarm philosophy.	Alarm data.
H	Monitoring & Assessment	Alarm system performance is measured and compared against KPIs from the philosophy. Problem alarms are identified (nuisance alarms, frequently occurring alarms).	Alarm data and alarm philosophy.	Alarm monitoring reports, proposed changes.
I	Management of Change	Process to authorize additions, modifications, and deletions of alarms.	Alarm philosophy, proposed changes.	Authorized alarm changes.
J	Audit	Periodic audit of alarm management processes (e.g., comparing DCS alarm settings to the Master Alarm Database)	Standards, alarm philosophy and audit protocol.	Recommendations for improvement.

7.1 Alarm Philosophy

This is the basic planning step before designing any new alarm system or modifying an existing one. This step documents the objectives of the alarm system and the process to achieve them. The alarm philosophy reflects operations and maintenance work processes and serves as the base for alarm system requirements specifications (ASRS), which guides system design. It also gives the criteria for alarm prioritization, definitions of alarm classes, responsibilities for managing alarm systems, performance metrics, and reporting requirements.

Generally, the alarm philosophy serves as the framework to establish the criteria, definitions, principles, and responsibilities for all alarm management lifecycle stages. This is achieved by specifying items, including the methods for alarm identification, rationalization, monitoring, management of change, and audit to be followed. An alarm philosophy document facilitates:

- Consistency across the alarm system.
- Consistency with risk management goals and objectives.
- Agreement with good engineering practices.
- Design and management of the alarm system that supports an effective operator response.

7.1.1 Alarm Philosophy Contents

The detailed content of the alarm philosophy can vary between industries and from one location to another. The required and recommended contents of the alarm philosophy are:

1. *Purpose of the alarm system (required);*

   The alarm philosophy shall include the purpose and objectives of a process plant alarm system. Having the purpose and objectives clearly defined supports the alarm management lifecycle activities. This definition can facilitate the design, implementation, and maintenance of an effective alarm system

2. *Definitions (required);*

   The alarm philosophy shall include definitions of terms encountered in designing and improving an alarm system to ensure that all participants share a common understanding.

3. *References (recommended);*

   The alarm philosophy should include a list of appropriate references. References may be internal company documents (e.g., MOC procedure), external standards, or published material.

4. *Roles and responsibilities for alarm management (required);*

   The alarm philosophy shall establish responsibility for the activities of the alarm management lifecycle.

5. *Alarm design principles (required);*

   The alarm philosophy shall address the criteria for selection and principles for the design of alarms, consistent with the definition of an alarm. The criteria and principles should address the following:

   - The role of the alarm system in identifying approaches to unsafe or abnormal operation, warning of malfunctions, and prompting the operator of actionable changes in the process.
   - The methods to be used for alarm identification.
   - The alarm states (e.g., normal, acknowledged, shelved, etc.) that the facility will use.

6. *Alarm setpoint determination (recommended);*

   The alarm philosophy should guide the methods used to determine alarm setpoints. Alarm setpoint determination can use several inputs (e.g., consequence thresholds or complexity of the operator response).

7. *Prioritization method (required);*

   Consistent priorities aid the operator in deciding the order of response during a period with a high alarm rate. The alarm philosophy shall address the prioritization, including the following:

   - The basis for alarm prioritization (e.g., the severity of consequence, time to respond, etc.).
   - The metrics for alarm design (e.g., priority distribution).
   - The impact of classification on prioritization, if any.

8. *Alarm class definition (required);*

   Alarm classes are used to set common alarm management requirements (e.g., testing, training, monitoring, and audit requirements). An alarm may belong to more than one class. This section should include the definition of the alarm classes.

9. *Highly managed alarms (recommended);*

   Highly managed alarm (HMA) classes are classes of alarms that require more administration and documentation than others. Alarm philosophy shall define the criteria for assigning alarms to HMA classes if HMA is used. The designation of alarm classes as highly managed should be based upon one or more of the following:

   - Alarms critical to process safety (e.g., safety alarms).

- Alarms for personnel safety or protection.
- Alarms for environmental protection.
- Alarms for current good manufacturing practices.
- Alarms for commercial loss.
- Alarms for product quality.
- Alarms for process licensor requirements.
- Alarms for company policy.

10. *Rationalization (required);*

    Alarm philosophy shall list the criteria for assessing alarms and the information captured during rationalization.

11. *Alarm documentation (required);*

    The alarm philosophy shall specify the documentation/record required to be preserved/maintained throughout the whole alarm lifecycle. Moreover, define its retention time.

12. *Alarm design guidance (required);*

    The alarm philosophy shall guide the design practices. This guidance should address the following:

    - Alarm Deadband.
    - Alarm on-delay.
    - Alarm off-delay.
    - Alarm types.
    - Composition of alarm messages.

13. *Specific alarm design considerations (recommended);*

    The alarm philosophy should specify rules and methods for the design of alarms covering specific circumstances where consistency is important (e.g., bypass alarms, alarms from redundant sensors, alarms from packaged systems, batch process-related alarms). Alarm classes may be the source of such specific design considerations.

14. *HMI design principles (required);*

    The alarm philosophy shall specify the alarm presentation method to establish consistent display and annunciation principles. Specific elements that should be covered in this section include the following:

    - Alarm presentation method (e.g., color, symbol, and alpha-numeric).

- The mechanism used (e.g., panel, BPCS console screens, etc.) to communicate the alarms to the operator.
- Recommendations for the indications on the HMI of the alarm states (e.g., normal, acknowledged, shelved, etc.) that will be used at the facility.
- Types of displays that will be used (e.g., alarm summary, first-out, etc.).
- Functions will be available in the HMI, including shelving, suppression, and enhanced and advanced alarm techniques.

15. *Approved enhanced and advanced alarming techniques (recommended);*

    The alarm philosophy will identify the approved techniques, related responsibilities, and work processes if enhanced and advanced alarming techniques are used.

16. *Implementation guidance (required);*

    The alarm philosophy shall specify the methods for initial training, commissioning, and checkout of the alarm system.

17. *Alarm response procedures (required);*

    The alarm philosophy shall address alarm response procedures. Available alarm response procedures can reduce the time it takes the operator to diagnose the problem (causes and consequences), determines the appropriate corrective action, and promote consistency between operators.

18. *Training (required);*

    The alarm philosophy shall address how plant personnel is to be trained on the use, management, and design of the alarm system, including the training documentation requirements.

19. *Alarm shelving (recommended);*

    The alarm philosophy should include guidance on how and when alarm shelving can be used, who can perform shelving, and authorization and documentation requirements. There are typically limits on which alarms can be shelved and shelving duration based on class or priority.

20. *Alarm system maintenance (required);*

    The alarm philosophy shall specify the activities necessary to maintain the alarm system.

21. *Testing of alarms (required);*

    The alarm philosophy shall address testing using alarm classes or other methods.

22. *Alarm system performance monitoring (required);*

    The alarm philosophy shall specify methods for assessing alarm system performance. Specific elements that shall be covered in this section include the following:

- The objective for monitoring and assessment.
- Monitoring metrics and target values.
- Guidance on the frequency of reviewing alarm system performance.
- Guidance on the approach to improve performance on the metrics.

23. *Alarm history preservation (recommended);*

    The alarm philosophy should specify the retention of alarm-related records (e.g., annunciations, acknowledgments, return to normal, and operator actions).

24. *Management of change (required);*

    The alarm philosophy shall identify the types of changes and the applicable MOC procedure. The MOC procedure ensures that changes made during design, implementation, operation, or maintenance are appropriately evaluated, authorized, and documented. This typically includes documented assessment, a description of each change, and authorization. Types of changes may include:

    - Temporary changes to alarms (e.g., out of service).
    - Permanent changes to the master alarm database, alarm attributes, or enhanced and advanced alarming techniques.

25. *Alarm management audit (required);*

    The alarm philosophy shall specify the requirements of periodic alarm management audits. These requirements may include audit frequency, specified based on alarm class, audit topics, and process for operator interviews.

26. *Related site procedures (recommended);*

    The alarm philosophy should reference relevant procedures. The following documents can be related to the alarm philosophy: standard operating procedure, training policies, and guides, HSE procedures, maintenance procedures, alarm handling policy, MOC procedure, etc.

7.1.2 Alarm Philosophy Development

Personnel who apply the alarm philosophy should be involved in developing the alarm Philosophy. The team involved should be equipped with detailed knowledge and understanding of the design, operation, and maintenance of the process related to the site. Specific areas of expertise include:

- Process operations.
- Process instrumentation.
- Control systems.
- Process technology.

- Mechanical/reliability engineering.
- Safety, health, and environment.
- Process safety.
- Human factors.
- Alarm management.
- MOC process.

7.2 Identification

Simply it is the collection stage of the potential alarms using several methods for determining that an alarm may be necessary. A variety of good engineering practices or regulatory requirements may identify alarms. Some combination of identification methods should be used to determine potential alarms. The alarm identification method may affect the classification of an alarm. Where appropriate, alarm identification may be done during alarm rationalization. The following is a list of the common methods that are used for alarm identification:

- Allocation of safety layers.
- Process hazards analysis (PHA).
- Hazard and operability study (HAZOP).
- Layer of protection analysis (LOPA).
- Incident investigations.
- Environmental permits.
- Failure mode and effects analysis (FMEA).
- Current good manufacturing practices.
- Quality reviews.
- P&ID reviews.
- Operating procedure reviews.
- Packaged equipment manufacturer recommendations.

The information related to potential alarms should be captured during identification and used in alarm rationalization, including consequence threshold, operator response, a consequence of inaction, probable cause, and rationale for consequence threshold.

7.3 Rationalization

In this stage, the identified need (from the identification stage) for an alarm or alarm system change is systematically compared to the criteria for alarm outlined in the alarm philosophy, as illustrated in Figure 5.

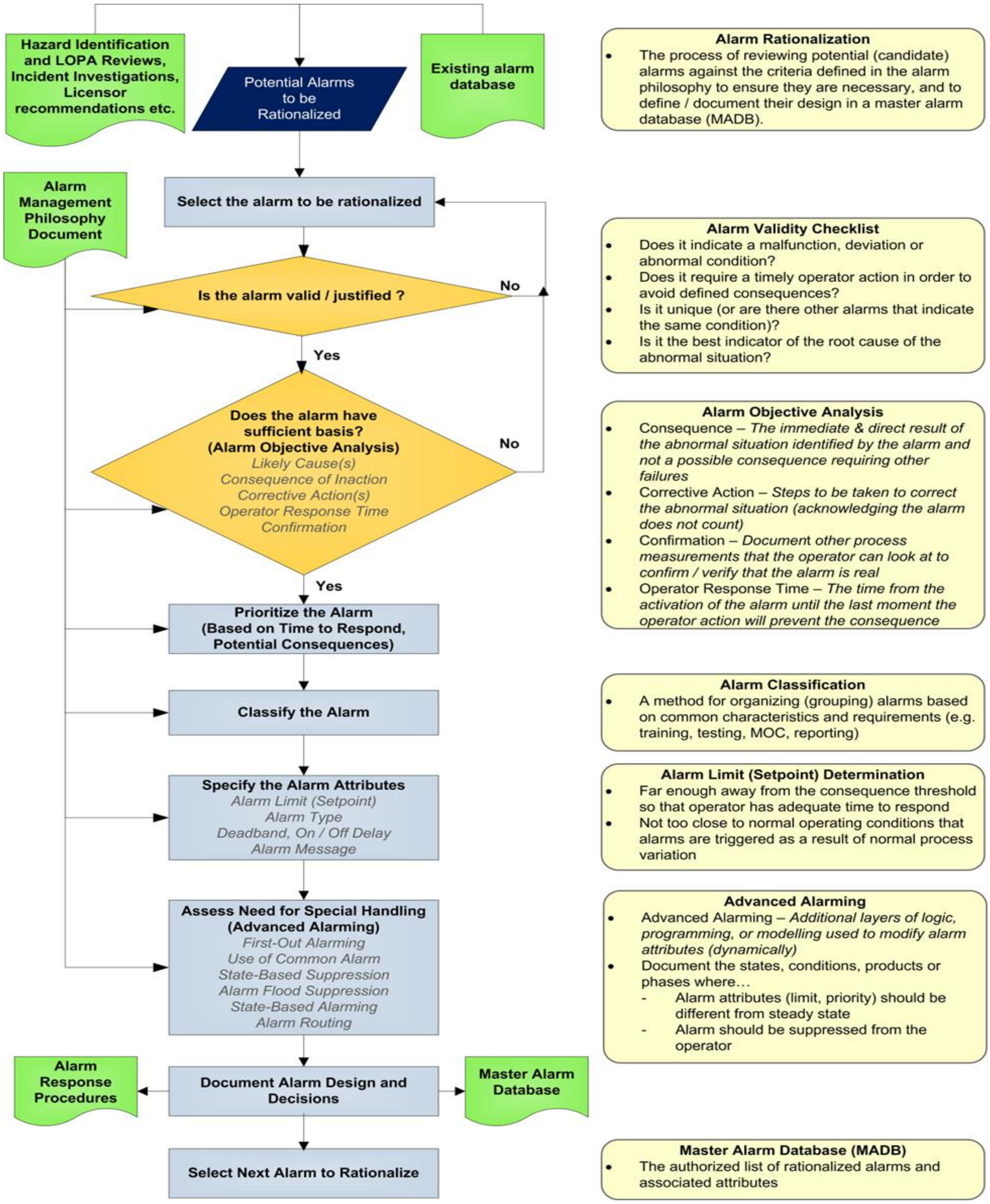


Figure 5. *Alarm rationalization process [2].*

If the proposed alarm meets the criteria, the alarm setpoint, consequence, and operator action are documented, and the alarm is prioritized and classified according to the philosophy. Rationalization produces the detailed design information documented in the master alarm database (MADB), which is necessary for the design stage of the alarm management lifecycle. The rationalization stage results are detailed design information necessary for the design stage. This information should include, as a minimum, the following: alarm type, priority, alarm class, alarm set point, operator action, a consequence of inaction or incorrect action, probable cause, and need for advanced alarming techniques if necessary.

Typically, the following activities are included in this stage: alarm justification, alarm setpoint determination, alarm prioritization, and alarm classification. Upon completion of the initial justification, prioritization, and classification of all the required alarms, the results should be reviewed to ensure consistent application of the criteria throughout the process. The results should be compared to any targets for the number and priority of alarms that might be documented in the alarm philosophy.

7.3.1 Alarm Justification

Every alarm requiring rationalization is compared to the pre-decided criteria in the alarm philosophy to justify that it is an alarm. These criteria include:

- The alarm is directed to the operator.
- The alarm indicates a process deviation, abnormal condition, or equipment malfunction.
- The alarm requires a timely response.

The alarm justification process utilizes a team approach, including knowledge of the process and the control system, and relies heavily upon operator inputs. All alarms to be rationalized are systematically reviewed, and the information to be captured for each rationalized alarm should be specified in the alarm philosophy and typically includes:

- Verification that the proposed alarm meets the criteria for an alarm stated in the philosophy.
- Action(s) the operator may take in response to the alarm.
- The consequence that will occur if action is not taken or is unsuccessful.
- Allowable response time.

Moreover, the alarm justification process should verify that the alarm will not become a nuisance and not duplicate another alarm. These negative conditions can be prevented by using advanced alarming techniques.

7.3.2 Alarm Setpoint Determination

Guidance for determining alarm setpoints is applied in the alarm philosophy. Effective methods use information including:

- Allowable response time.
- The complexity of the operator action.
- The time necessary to complete the operator action.
- Normal operating range.
- Other operating or design boundaries.
- Knowledge of the process operation and history.

7.3.3 Prioritization

Alarm priority is used to aid the operator in determining the order in which to respond to alarms. The method for priority assignment defined in the alarm philosophy is applied to the rationalized alarm, and a priority is assigned. Effective prioritization typically results in higher priorities being chosen less frequently than lower priorities. Most of the alarms should be assigned to the lowest alarm priority (least important) and the fewest to the highest alarm priority (most important), with a consistent transition between the two. The resulting priorities should have alignment with the consequence and allowable response time, such that the lowest priority alarms have the least severe consequences and longest allowable response times, and the highest priority alarms have the most severe consequences (e.g., fire and gas alarms) and the shortest allowable response times. Prioritization may include consideration for alarm classes (e.g., High managed alarm (HMA) classes) or identification methods (e.g., LOPA) to set alarm priority.

7.3.4 Classification

Alarms shall be assigned to one or more classes defined in the alarm philosophy. It is important to mention that alarms in the same class are not required to have the same priority.

7.3.5 Documentation

Rationalization shall be documented to become the basis for ensuring the integrity of the alarm system. The documentation (e.g., MADB) is the link between each alarm and the alarm philosophy and can be used for several purposes, including:

- Input to the detailed design stage of the alarm lifecycle.
- Utilization as part of the MOC.
- Alarm response procedures.
- Training of and use by operators.

- Periodic auditing and reconciliation of the control system alarm settings.
- Evaluation of alarm monitoring and effectiveness data.

7.4 Detailed Design

In this stage, additional alarm attributes are specified and designed in light of the result of alarm rationalization. This design stage includes:

- Basic alarm design: The basic design for each alarm follows guidance based on the type of alarm and the specific control system.
- HMI design: The HMI design includes display and annunciation for the alarms, including the indications of alarm state and alarm priority.
- Advanced alarming system design: Advanced alarming techniques are additional functions that improve the effectiveness of the alarm system beyond the basic alarm and HMI design (e.g., state-based alarming).

7.4.1 Basic Alarm Design

Basic alarm design is part of the detailed design stage in which design considerations to implement the alarms within a specific control system are addressed as specified by the rationalization process. In this respect, the capabilities of the control system should be considered.

Changes in alarm state can be triggered from various sources within a control system, including field devices (sensors and final control elements), the control and safety system, and HMI. The source for each alarm in the system should be documented.

Clear design guidance should be provided whenever alarm state information is used with other logic functions (e.g., interlock actions). If alarm setpoints are used in addition to operator notification (e.g., as an interlock setpoint), then documentation, training, and change management can be impacted. Additionally, the impact of modifying alarm attributes and the use of designed suppression should be clearly identified, documented, and potentially restricted (e.g., extra confirmation or higher access level required). This information should be specifically documented in the alarm philosophy under alarm design principles.

An alarm type should be assigned to each alarm defined during rationalization. The alarm type is defined to give the operator a visual distinction of the alarm. The alarm type shall be implemented based on the information documented in the master alarm database. The common alarm types may include the following: absolute alarms, deviation alarms, rate-of-change alarms, discrepancy alarms, calculated alarms, recipe-driven alarms, bit-pattern alarms, controller output alarms, system diagnostic alarms, instruments diagnostic alarms, adjustable alarms, re-alarming alarms, statistical alarms, first-out alarms, and bad-measurement alarms.

The available alarm types that are included within a control system can vary. It could be necessary to create a custom alarm type as part of the engineering scope of a project. Alarms may be of a single type or a combination of types. Alarm types should be selected carefully based on engineering judgment. Certain types, such as rate-of-change, deviation, bad-measurement, and controller output alarms, can be sources of nuisance alarms if they are not applied appropriately.

During the basic design process, the default alarm attributes should be configured for each alarm that has been rationalized and set based on engineering judgment. Attributes such as setpoint and deadband can differ depending on the specific alarm type implemented. Defining appropriate alarm attributes can help minimize the number of nuisance alarms generated during operation. Alarm attributes should include alarm description, alarm setpoint or logical conditions, alarm priority, alarm Deadband, on-delay or off-delay, alarm group, and alarm message. Programmatic changes to alarm attributes could occur to respond to specific conditions such as a batch recipe, product type, or grade. Alarm attributes can typically be modified from one or more of the following sources:

- Operator interface (e.g., manual changes during operation).
- Engineering interface (e.g., design changes under the management of change).
- The control logic (e.g., sequences, phases).
- Advanced alarming techniques.
- External to the control system (e.g., manufacturing execution system (MES), enterprise resource planning (ERP) system).

The alarm philosophy should detail the use and limitations of this functionality. For each alarm, the user should identify and document which programs of the system will have access to modify alarm attributes during operation and which changes will be subject to the management of change procedures.

A typical control system allows the user to implement numerous different alarm types for a single process variable. To minimize alarm loading on the operator, the basic alarm design results should be reviewed against the master alarm database to ensure that only the required alarms exist.

7.4.2 Human-Machine Interface (HMI) Design for Alarm Systems

The HMI design for alarm systems is part of the detailed design stage. The indication and display of alarms is only one component of the HMI design and contributes to effective operator-process interaction. The HMI design for alarms should be consistent with the alarm philosophy and the overall HMI design philosophy. The capabilities of the control system should be considered in the HMI design. Generally, the HMI shall indicate the unsuppressed active alarms, alarm states, alarm priorities, and alarm types.

An HMI independent from the BPCS may be required for the following safety alarms: safety-related alarms, depending on considerations (e.g., the risk reduction factor), and system diagnostic alarms from the SIS that indicate dangerous faults, depending on considerations (e.g., the operator response, communication fault).

The HMI should be designed to provide the ability to silence audible alarm indications, acknowledge alarms, place alarms out of service through allowable access control, modify alarm attributes through allowable access control, initiate an alarm shelving function, support a designated suppression function, and display alarm messages.

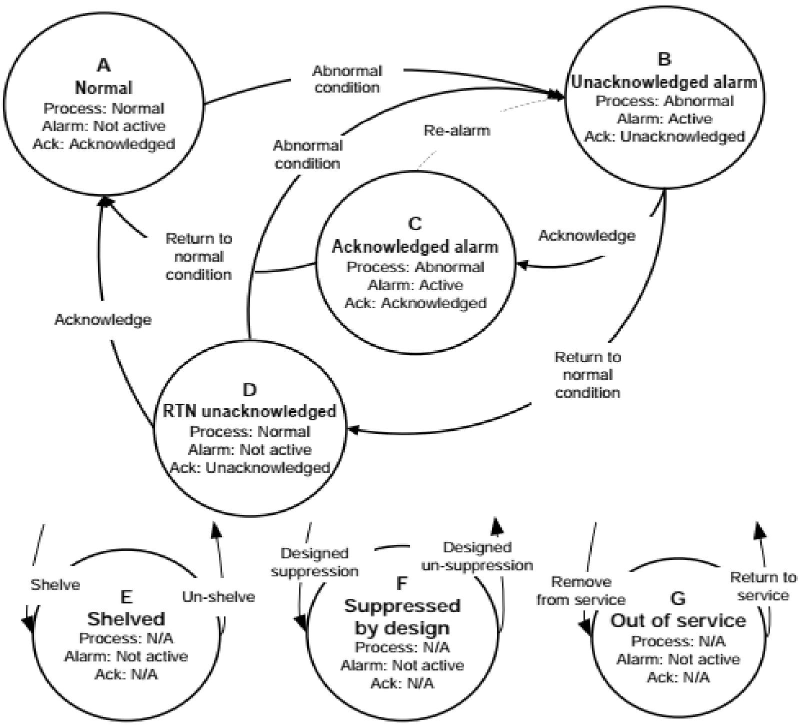
Also, the design of the HMI shall provide the following capabilities or equivalent: alarm summary displays, alarm indications on process displays, alarm indications on tag detail displays, shelved alarm summary displays, suppressed-by-design summary displays, out-of-service summary displays, and system diagnostic alarm displays.

The HMI design shall support retrieving the alarm records, which is a set of information that documents the alarm state change. An alarm record should have the following attributes: tag the name for the alarm, tag description or alarm description for the alarm, alarm state, alarm priority, alarm type, and time & date of occurrence of alarm state change. Moreover, the alarm record should have the following elements: process value at the time of alarm, alarm setpoint, alarm group or process area, alarm class, and alarm message.

A combination of visual indications, audible indications, or both, shall be used to uniquely distinguish the following typical alarm states: normal, unacknowledged alarm, acknowledged alarm, and return to normal unacknowledged alarm. The alarm state transition diagram shown in Figure 6 represents the states and transitions for typical alarms. While there are exceptions, this diagram describes most alarms and is a useful reference for developing alarm system principles and HMI functions.

- **Normal state (A)**: The normal (NORM) alarm state is defined as the state where the process operates within normal specifications, the alarm is inactive, and past alarms have been acknowledged.
- **Unacknowledged state (B)**: The unacknowledged alarm (UNACK) state is the initial state of an alarm becoming active due to abnormal conditions. In this state, the alarm is unacknowledged. Previously acknowledged alarms can be designed to re-alarm, causing a return to this state.
- **Acknowledged state (C)**: The acknowledged (ACKED) alarm state is where the alarm is active, and the operator has acknowledged the alarm.
- **Return to normal unacknowledged state (D)**: In the returned to normal unacknowledged (RTNUN) alarm state, the process is within normal limits, and the alarm becomes inactive before an operator has acknowledged the alarm condition.

- **Shelved state (E)**: In the shelved (SHLVD) alarm state, an alarm is temporarily suppressed using a controlled methodology and not annunciated. An alarm in the shelved state is under the control of the operator. The shelving function can automatically unshelve alarms.
- **Suppressed-by-design state (F)**: In the suppressed–by-design (DSUPR) alarm state, an alarm is suppressed based on operating conditions or plant states and not annunciated. An alarm in the suppressed-by-design state is under the control of logic that determines the relevance of the alarm.
- **Out-of-service state (G)**: In the out-of-service (OOSRV) alarm state, an alarm is manually suppressed (e.g., control system functions to remove the alarm from service) when it is removed from service, typically for maintenance, and not annunciated. An alarm in the out-of-service state is under the control of maintenance.



NOTE 1: States E, F, and G can connect to any alarm state in the diagram.
NOTE 2: the dotted line indicates an infrequently implemented option.

***Figure 6.** Alarm state transition diagram.*

Alarm priorities are used in the HMI to assist the operator in selecting the sequence of alarm response actions. A unique combination of visual indications, audible indications, or both, shall be used to distinguish the alarm priorities within the alarm system.

The alarm message further clarifies the alarm beyond the tag name, state, and priority indication. It may also include part of the operator's action or a reference to the alarm response procedure. The common industry practices to indicate alarm messages are visual alarm message indications and vocalized alarm message indications.

7.4.3 Design of Advanced Alarming System

Enhanced and advanced alarming is part of the detailed design lifecycle stage. It considers additional alarm management techniques beyond those normally employed in control systems. They generally provide added functionality over the basic alarm system design and are particularly useful to guide operator action during abnormal process conditions. Enhanced and advanced alarming methods are additional logic, programming, or modeling layers used to modify alarm attributes. Advanced alarming modifies alarm behaviors, including logic-based, dynamic, state-based alarming (i.e., mode-based alarming), and adaptive alarms. Most designed suppression methods are included in advanced alarming. In addition to advanced alarming techniques, enhancements to the alarm system provide additional information to the operator or redirect the alarm to the designated responder. The basic alarm design methods may not be sufficient to reduce alarm floods or mitigate their effect, so enhanced and advanced techniques may be necessary. The methods described can reduce or eliminate floods.

To maintain the designed alarm attribute settings (e.g., alarm setpoints and alarm priorities) at authorized values, there should be a regular comparison of the rationalized values with the settings in effect in the control system. Enforcement, the automatic verification, and restoration of alarm attributes is an enhanced alarm technique that performs monitoring, assessment, and audit functions. Enforcement can be initiated on a scheduled basis or request and should differentiate changes resulting from state-based alarming or alarm shelving methodologies.

The alarm philosophy should specify steps to ensure advanced alarming techniques continue to operate, including training, testing, and auditing. Accordingly, training, testing, and auditing procedures should include enhanced and advanced alarming techniques.

7.5 Implementation

The implementation phase is a transition from design to operation. This stage should consider disruptions to operation, functional testing or validation, verification of documentation, and operator training.

Implementation testing requirements for new alarms and modifications to existing alarms are determined by the alarm classification and class requirements as detailed in the alarm philosophy. The testing should include verification of the following: alarm setpoint, alarm priority, audible and visual indications, and any other functional requirements as specified.

Operators are an essential part of the alarm system; operator training is an important activity during implementation. The training requirements for new alarms and modifications to existing alarms are determined by the classification of the alarm and the class requirements as detailed in the alarm philosophy. Operators shall be trained to respond to new or modified alarms prescribed in the alarm philosophy or site MOC procedure. The training requirements for the modified alarm system should be appropriate for the nature of the change. The training requirements of the new alarm system should include the following:

- Audible and visual indications for alarms.
- Methods for silencing an alarm.
- Methods for acknowledging an alarm.
- The distinction of alarm priorities.
- Use of the alarm HMI features (e.g., alarm summary sorting and filtering).
- Methods for shelving and suppression.
- Methods for removing an alarm from service.

Training, testing, and commissioning documentation can vary with classification as defined in the alarm philosophy. In general, the following documentation should be provided during the implementation phase:

- Rationalization information.
- Sufficient information to perform testing of alarms.
- Alarm response procedures.
- Any designed suppression or enhanced alarming documentation.
- Test documentation, if required by the alarm philosophy.

7.6 Operation

In this stage, the alarm system is becoming handover to the operator, and it becomes in service where it performs its intended function. The stage also might include refreshment training for the alarm philosophy and each alarm's purpose. In this stage, the alarm response procedures should be readily accessible to the operator as specified in the alarm philosophy. Indeed, the alarm information recorded during the rationalization phase should also be made readily accessible.

Unless otherwise specified in the alarm philosophy, the alarm response procedure should include the following: tag name of the alarm, tag description for the alarm, alarm type, alarm setpoint, potential causes, consequences of inaction, operator action, allowable operator response time, and alarm class.

During operation, careful consideration should be devoted to alarm shelving. If a highly managed alarm class is used, then shelving highly managed alarms shall follow authorization and reauthorization requirements as detailed in the alarm philosophy. Documentation shall be maintained, including approval, interim alarms and procedures, and reauthorization details. It should be reviewed whenever shelved alarms extend beyond a single operating shift. The reviewing procedure should be documented in the alarm philosophy.

As mentioned before, during the operation phase, the operators should receive refresher training that involves alarm response procedures. The refreshing training should include rationalization information about the alarm and the audible and visual indications for the alarm. A record for refreshment training should be maintained indicating who received the training and the time it was received.

7.7 Maintenance

This stage covers the requirements for alarm system testing, replacement, and repair activities. This stage might also include a consideration of refresher training for the maintenance staff on the alarm system. Periodic alarm testing requirements shall be determined by the alarm classification or other methods as detailed in the alarm philosophy. Test procedure should be provided, containing information related to the testing methodology and the planned interval before the next test. Moreover, the testing procedure must have information related to the following:

- Steps for taking the alarm out of service before the test and returning the alarm to service after the test, including notification to the operator.
- Appropriate warnings regarding control loops or final elements that might be affected by the test.
- Steps to address advanced alarming techniques if applicable.

The purpose of periodic testing is to ensure that the alarm continues to perform as designed. Once the tests are performed, a record should be maintained for a period as specified by the alarm philosophy. These records should include the following information: date of testing, the person(s) who performed the tests, identification of tested equipment or item, test procedure, test results, causes of test failures, and next test date.

If the test resulted in deficiencies, they should be fixed/repaired promptly. Information related to an alarm malfunction should be available to the operator. Alarms affected by non-functioning equipment (e.g., equipment taken out of service for repair or preventative maintenance) should be placed out of service if the condition is not resolved within a reasonable time, as specified in the alarm philosophy. Whenever the situation requires getting alarms out of service accordingly, specific requirements for out-of-service procedures shall be determined by the alarm classifications or other methods as detailed in the alarm philosophy. These requirements should focus on the required permits and level of authorization and documentation process of out-of-service alarm(s). If a highly managed alarm is taken out of service, appropriate interim alarms or procedures shall be identified considering risk reduction requirements and the plant state. Before returning out-of-service alarms to the operational state, operators shall be notified to ensure they are aware of the returning alarm and the removal of the interim methods. Interim alarms and procedures shall be removed, where applicable, when the original alarms are returned to service. Finally, a record shall be maintained, including the following information for any out-of-service alarm: alarm name/tag/type, approval details, reasons for taking the alarm out of service, and details concerning interim alarms or procedures if required.

Maintenance activities might include replacement activities; whenever there is a replacement of equipment (e.g., measurement devices, valves, process equipment) that will change the alarm attributes, it should be handled through the management of the change procedure. In such replacement cases, alarm validation may be required depending on the class of the alarm as specified in the alarm philosophy.

Maintenance personnel should receive refresher training on the maintenance requirements of alarms. A record of refresher training should be kept indicating who received the training and the time it was received. Evaluations should be conducted to ensure site maintenance procedures are clearly understood.

7.8 Monitoring and Assessment

In this stage, the alarm system and each alarm are continuously monitored and periodically assessed against the performance goals mentioned in the alarm philosophy. Monitoring and assessing the data from the operation stage may trigger maintenance work or identify the need to modify the alarm system or operating procedures. Without this stage, alarm system degradation over time is highly possible.

Once the alarm management lifecycle has been implemented and nuisance alarms (e.g., chattering alarms) reduced, the resulting alarm rate more closely reflects the effectiveness of the control of the process, the operating practices, and the maintenance systems. Alarm system performance can be further improved through process control, operation, or maintenance improvements. Advanced alarm techniques are often necessary to meet the performance targets in the alarm philosophy.

Monitoring typically occurs at a higher frequency than assessment. Monitoring some aspects of the alarm system performance is based upon continuous measurement. Monitoring intends to identify problems and take corrective actions to fix them. On the other hand, the focus of the assessment process is to apply engineering judgment about the system's performance. The list of chosen analyses should match the alarm philosophy. The two categories of data in a typical alarm system are:

- Alarm records (i.e., dynamic, or real-time data) contain alarm-related information and are produced by the system when alarms occur.

- Alarm attributes make up the underlying structure necessary to produce alarm records, including alarm types, alarm setpoints, priorities, deadbands, and similar items.

Both categories are valuable in alarm system performance measurement and are subject to different analyses. Alarm system analyses should be reported at the appropriate frequency to personnel (e.g., operators, staff, and managers) concerned with the alarm system. The alarm philosophy should specify analysis and reporting frequencies. Action should be taken on problems identified by the alarm analyses. The progress and status of actions should be regularly reported.

7.8.1 Alarm System Performance Metrics

Various alarm system analyses, key performance indicators, and methods are possible. Both initial alarm system assessment and ongoing monitoring should include the measures like those shown in Table 2.

Table 2. *Recommended alarm performance metrics summary.*

Alarm Performance Metrics Based upon at least 30 days of data		
Metric	**Target Value**	
Annunciated Alarms per time	Target Value: Very Likely to be Acceptable	Target Value: Maximum Manageable
Annunciated Alarms Per Day per Operator Console	~144 alarms per day	~288 alarms per day
Annunciated Alarms Per Hour per Operator Console	~6 (average)	~12 (average)
Annunciated Alarms Per 10 Minutes per Operator Console	~1 (average)	~2 (average)
Metric	**Target Value**	
Percentage of hours containing more than 30 alarms	~<1%	
Percentage of 10-minute periods containing more than 10 alarms	~<1%	
Maximum number of alarms in a 10-minute period	≤10	
Percentage of time the alarm system is in a flood condition	~<1%	
Percentage contribution of the top 10 most frequent alarms to the overall alarm load	~<1% to 5% maximum, with action plans to address deficiencies.	
Quantity of chattering and fleeting alarms	Zero, action plans to correct any that occur.	
Stale Alarms	Less than 5 present on any day, with action plans to address	
Annunciated Priority Distribution	3 priorities: ~80% Low, ~15% Medium, ~5% High or 4 priorities: ~80% Low, ~15% Medium, ~5% High, ~<1% "highest" Other special-purpose priorities (e.g. system diagnostic alarms) excluded from the calculation.	
Unauthorized Alarm Suppression	Zero alarms suppressed outside of controlled or approved methodologies.	
Unauthorized Alarm Attribute Changes	Zero alarm attribute changes outside of approved methodologies or MOC	

7.8.1.1 Average Alarm Rate per Operator Console

Analysis of the alarming rate (i.e., annunciated alarm rate) is a good indicator of the overall health of the alarm system. Recommended targets for the average alarm rate per operator console based on one month of data are shown in Table 2. These rates are based upon the ability of an operator and the time necessary to detect an alarm, diagnose the situation, respond with corrective action(s), and monitor the condition to verify the abnormal condition has been corrected.

7.8.1.2 Peak Alarm Rate per Operator Console

Alarm rates can exceed the operator's capability for effective alarm response (e.g., 10 alarms or more in 10 minutes) and result in missed alarms. For peak alarm rate analysis, annunciated alarms are counted in regular 10-minute intervals. The recommended target corresponding to one month of data is that less than ~1% of the 10-minute intervals should contain more than 10 alarms. The peak and average alarm rates should be considered simultaneously because either measurement could be misleading. The number of intervals exceeding 10 alarms and the magnitude of the highest peaks should be reported.

7.8.1.3 Alarm Floods

Alarm floods are variable-duration periods of alarm activity with annunciation rates likely to exceed the operator response capability. Alarm flood calculations involve determining adjacent periods where the alarming rate is high, thus producing an overall flood event. A high alarm rate indicates the start of an alarm flood (e.g., an alarming rate that exceeds 10 alarms per 10 minutes), and the end of an alarm flood is indicated by a return to a reduced alarm rate (e.g., an alarming rate of fewer than 5 alarms per 10 minutes). Alarm floods should be of short duration and have a low total alarm count. As a recommended target, an alarm system should be in flood for less than ~1% of the time.

Alarm flood analysis should include the following:

- Number of alarm floods.
- Duration of each alarm flood.
- Alarm count in each alarm flood.
- Peak alarm rate for each alarm flood.

In general, the analysis of alarm floods may indicate improvements to the alarm system and process operation. Alarm floods may require advanced methodologies to address.

7.8.1.4 Frequently Occurring Alarms

Few individual alarms (e.g., 10 to 20) often produce a large percentage of the total alarm system load (e.g., 20% to 80%). The most frequent alarms should be reviewed at regular intervals (e.g., daily, weekly, or monthly). Substantial performance improvement can be made by addressing the most frequent alarms. The top 10 most frequent alarms should comprise a small percentage of the overall system load (e.g., 1% to 5%). Action steps based on this analysis include a review for correct functioning and design.

7.8.1.5 Chattering and Fleeting Alarms

A chattering alarm repeatedly transitions between the active and not active states in a short time. Fleeting alarms are similar to short-duration alarms that do not immediately repeat. In both cases, the transition is not due to the result of operator action.
A chattering alarm can generate hundreds or thousands of records in a few hours. This results in a significant distraction for the operators. Chattering alarms are often high in the listing of the most frequent alarms. Chattering and fleeting alarm behaviors should be eliminated. There is no acceptable long-term quantity of chattering or fleeting alarms.

7.8.1.6 Stale Alarms

Alarms that remain annunciated continuously for an extended duration (e.g., longer than 24 hours) can be considered stale. Such alarms provide little valuable information to the operators. Stale alarms should be examined to ensure that they are properly rationalized. Advanced alarming or resolving the root cause can eliminate stale alarms. There should be a few stale alarms per operator console, with action plans to address them. No alarm should be intentionally designed to become stale, and there is no acceptable long-term number of stale alarms.

7.8.1.7 Annunciated Alarm Priority Distribution

Effective use of alarm priority can enhance the ability of the operator to manage alarms and provide a response. The effectiveness of alarm priority is related to the distribution of the alarm priorities: higher priorities should be used less frequently. Alarm priority distributions can vary based on process and industry. A target alarm priority distribution should be established in the alarm philosophy. Significant variance from the target priority distribution can indicate ineffective rationalization or ineffective application of the alarm prioritization methodology.

An effective alarm rationalization effort will produce an annunciated alarm priority distribution similar to the target distribution in the alarm philosophy. The annunciated alarm priority distribution will not match the rationalized alarm priority distribution since all alarms are not equally likely to occur. For alarm systems that do not allow a separate priority for instrument or system diagnostic alarms, these alarms can be excluded from the priority distribution calculations to prevent a skewed distribution.

7.8.2 Unauthorized Alarm Suppression Monitoring

The shelved, suppressed-by-design and out-of-service alarm states are all intended as controlled methodologies. Alarms can be suppressed outside of these methodologies. Unauthorized suppression of alarms should be detected and reported. The potential for mistakes and the resulting risk are high. Alarm state transitions to suppressed states and from suppressed states should be recorded. Analysis methods should be used to detect and report any alarms suppressed outside of these methods. There should be no alarms that are suppressed without authorization.

7.8.3 Alarm Attribute Monitoring

Unauthorized alarm attribute changes shall be detected and resolved by comparison of actual alarm attributes against rationalization information. Discrepancies shall be identified and resolved quickly. The target value for unauthorized changes to alarms is zero.

7.9 Management of Change

This stage is about the process for alarm system changes pertaining to adding new alarms, removing existing alarms, alarm attribute modification, authorization, and documentation. This change process should follow the normal alarm management lifecycle stages from identification to implementation.

The addition or removal of alarms and the modification of specified attributes shall require authorization through the management of the change procedure. Permanent changes that result in a difference from the authorized values of the alarm setpoint, class, priority, consequence, basis, suppression logic, or response time shall require evaluation through the management of change (MOC) procedure.

The applied MOC for alarm system changes shall address the following considerations:

- The technical basis for the proposed change.
- Impact of change on health, safety, and the environment.
- Modifications are per the alarm philosophy.
- Modifications for operating procedures.
- The period for which change is valid.
- Authorization requirements for the proposed change.
- The degree of safety is maintained if the alarm is implemented for safety reasons.
- Personnel from appropriate disciplines are included in the review.
- Changes to the alarm system follow all appropriate subsequent alarm management lifecycle activities.

- Implementation of all changes adheres to procedures specified in the alarm philosophy.

Finally, Changes required to related system components and documentation because of alarm changes should be recorded as part of the change record. Typically, the following information shall be recorded for approved changes:

- Reason for the change.
- Date of change.
- The person implementing the change.
- The person authorizing the change.
- Nature of the change (i.e., the before and after).
- Training requirements.
- Testing requirements.

7.10 Audit

In this stage, a periodic review is conducted to ensure the effectiveness of the alarm management process and maintain the integrity of the alarm system. The audit frequency and the specific audit requirements stated in the alarm philosophy shall be followed for all alarms, as required by alarm class or other methods.

The audit should address all applicable requirements stated in this guideline. The audit frequency and the specific audit requirements stated in the alarm philosophy shall be followed for all alarms, as required by the alarm class. Personal interviews or questionnaires should be conducted as part of the audit to identify the performance and usability issues.

Action plans should be developed for problems identified during the audit processes. When defining an action plan, timelines, accountability, and review of results obtained should be assigned to each item. The alarm philosophy document may need to be modified to reflect changes resulting from the audit process.

8. References

[1] ANSI/ISA-18.2-2016, Management of Alarm Systems for the Process Industries.

[2] EXIDA, The ISA-18.2 Alarm Management Lifecycle,2011.

[3] International Electrotechnical Commission, IEC 62682 Management of Alarm Systems for the Process Industries. IEC, Geneva, Switzerland. 2014.

[4] EEMUA, Alarm Systems-A Guide to Design, Management, and Procurement. EEMUA Publication. 2013; 191.

[5] API RP. 1167, Pipeline SCADA Alarm Management, Second Edition, June 2016.

[6] Goel P, Datta A, Mannan MS. Industrial alarm systems: Challenges and opportunities. Journal of Loss Prevention in the Process Industries. 2017.

[7] HSE G. The Explosion and Fires at the Texaco Refinery, Milford Haven, 24 July 1994: A Report of the Investigation by the Health and Safety Executive Into the Explosion and Fires on the Pembroke Cracking Company Plant at the Texaco Refinery, Milford Haven on 24 J. Incident Report Series.

[8] Wilkinson J, Lucas D. Better alarm handling—a practical application of human factors. Measurement and control. 2002 Mar; 35(2):52-4.

[9] Rothenberg DH. Alarm Management for Process Control: A Best-Practice Guide for Design, Implementation, and Use of Industrial Alarm Systems. Momentum Press; 2018.

[10] Hollifield BR, Habibi E. The alarm management handbook: a comprehensive guide: practical and proven methods to optimize the performance of alarm management systems. Pas; 2010.

[11] Center for Chemical Process Safety (CCPS). Human Factors Handbook for Process Plant Operations: Improving Process Safety and System Performance. New York, NY: American Institute of Chemical Engineers; 2022.

[12] Wang J, Yang F, Chen T, Shah SL. An overview of industrial alarm systems: Main causes for alarm overloading, research status, and open problems. IEEE Transactions on Automation Science and Engineering. 2015.