Report

Philosophy of ITER Alarm System Management

Design, development, procurement, operation and maintenance of ITER alarms

Abstract

This guide provides simple and practical guidance to plant system Instrumentation and Control (I&C) responsible officers and designers on how to design, develop, procure, operate and maintain an effective plant system alarm system.

<table>
<thead>
<tr>
<th>Approval Process</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
</tr>
<tr>
<td>Author</td>
</tr>
<tr>
<td>Co-Authors</td>
</tr>
<tr>
<td>Reviewers</td>
</tr>
<tr>
<td>Approver</td>
</tr>
</tbody>
</table>

Document Security: level 1 (IO unclassified)

RO: Journeaux Jean-Yves

Read Access: AD: ITER, AD: External Collaborators, AD: Division - Control System Division - EXT, AD: Section - CODAC - EXT, AD: Section - CODAC, project administrator, RO, LG: CODAC team
<table>
<thead>
<tr>
<th>Title (Uid)</th>
<th>Version</th>
<th>Latest Status</th>
<th>Issue Date</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Philosophy of ITER Alarm System Management (3WCD7T_v2_1)</td>
<td>v2.1</td>
<td>Approved</td>
<td>01 Feb 2013</td>
<td>PCDH V7 schema</td>
</tr>
<tr>
<td>Philosophy of ITER Alarm System Management (3WCD7T_v2_0)</td>
<td>v2.0</td>
<td>Approved</td>
<td>10 Feb 2011</td>
<td>Reference to ITER process for Alarm System Development (ITER D 3UZXA2)</td>
</tr>
<tr>
<td>Philosophy of ITER Alarm System Management (3WCD7T_v1_1)</td>
<td>v1.1</td>
<td>Signed</td>
<td>05 Jan 2011</td>
<td>Internal Review Comments integrated.</td>
</tr>
<tr>
<td>Philosophy of ITER Alarm System Management (3WCD7T_v1_0)</td>
<td>v1.0</td>
<td>Approved</td>
<td>02 Dec 2010</td>
<td></td>
</tr>
</tbody>
</table>
Table of Contents

1 Introduction .............................................................................................................................. 3
  1.1 PCDH Context ....................................................................................................................... 3
  1.2 Document Scope ................................................................................................................... 4
  1.3 Related documents ............................................................................................................... 4
2 Benefits of alarm management .................................................................................................. 5
  2.1 Purpose of the alarm management ....................................................................................... 5
  2.2 Indicators of poor alarm management .................................................................................. 6
    2.2.1 Nuisance Alarms .............................................................................................................. 6
    2.2.2 Stale or Standing Alarms ............................................................................................... 6
    2.2.3 Alarm Floods .................................................................................................................. 6
    2.2.4 Alarm Clarity .................................................................................................................. 6
  2.3 What is an Alarm? ................................................................................................................. 6
  2.4 Alarm management lifecycle ............................................................................................... 7
    2.4.1 Philosophy ...................................................................................................................... 7
    2.4.2 Identification .................................................................................................................. 8
    2.4.3 Rationalisation ............................................................................................................... 8
    2.4.4 Detailed Design .............................................................................................................. 8
    2.4.5 Implementation ............................................................................................................. 8
    2.4.6 Operation ...................................................................................................................... 8
    2.4.7 Maintenance .................................................................................................................. 8
    2.4.8 Monitoring and Assessment ......................................................................................... 8
    2.4.9 Management of Change ............................................................................................... 8
    2.4.10 Audit ............................................................................................................................ 8
  2.5 Alarm Glossary .................................................................................................................... 9
3 Alarm philosophy principles ..................................................................................................... 10
  3.1 What is an Alarm System? .................................................................................................. 10
  3.2 The role of the operator ...................................................................................................... 10
  3.3 Characteristics of a good Alarm System ............................................................................. 11
  3.4 Key Design Principles ....................................................................................................... 11
  3.5 Context sensitive ................................................................................................................. 11
  3.6 Alarm for redundant components ...................................................................................... 12
  3.7 Dependant failures ............................................................................................................. 12
  3.8 Alarm Engineering Checklist ............................................................................................. 12
4 Rationalisation .......................................................................................................................... 13
5 Detailed Design ........................................................................................................................ 14
5.1 Limit Alarm ..............................................................................................................14
5.2 State Alarm .............................................................................................................16
5.3 Alarm HMI ..............................................................................................................16
  5.3.1 Alarm information in mimics .................................................................16
  5.3.2 Alarm Related Display .................................................................17
  5.3.3 Alarm Tree View ..................................................................................17
  5.3.4 Active Alarm View ..............................................................................17
  5.3.5 Acknowledged Alarm View .................................................17
  5.3.6 Message History .................................................................................17

6 Implementation ......................................................................................................17
  6.1 Alarm Testing .....................................................................................................17
  6.2 Training ..............................................................................................................17

7 Monitoring and assessment ..................................................................................18
1 Introduction

1.1 PCDH Context

The Plant Control Design Handbook (PCDH) [RD1] defines methodology, standards, specifications and interfaces applicable to ITER Plant Systems Instrumentation & Control (I&C) system life cycle. I&C standards are essential for ITER to:

- Integrate all plant systems into one integrated control system.
- Maintain all plant systems after delivery acceptance.
- Contain cost by economy of scale.

PCDH comprises a core document which presents the plant system I&C life cycle and recaps the main rules to be applied to the plant system I&Cs for conventional controls, interlocks and safety controls. Some I&C topics will be explained in greater detail in dedicated documents associated with PCDH as presented in Figure 1.1. This document is one of them.

![Figure 1.1 – Schema of PCDH documents](image-url)

Legend
This document
Available and approved
(IDM ref.)
1.2 **Document Scope**

This guide provides simple and practical guidance to plant system Instrumentation and Control (I&C) responsible officers and designers on how to design, develop, procure, operate and maintain a compliant and effective plant system alarm system.

1.3 **Related documents**


[RD3] ISA draft standard S18.02 - Management of Alarm Systems for the Process Industries,


[RD5] ITER process for Alarm System Development (ITER_D_3UZXA2 v1.1)
2 Benefits of alarm management

Any instrumented and controlled system may perform some or all of the following functions:

- Monitoring, recording and logging of plant system status and process parameters,
- Provision of operator information regarding the plant system status and process parameters,
- Provision of operator controls to affect changes to the plant system status,
- Automatic process control and batch/sequence control during start-up, normal operation, shutdown, and disturbance i.e. control within normal plant system operating limits,
- Detection of onset of hazards and automatic hazard termination i.e. control within safe plant system operating limits, or mitigation,
- Prevention of automatic or manual control actions which might initiate a hazard.

These functions are normally provided by different systems:

- The process control system,
- The protection system (trip, interlocks and emergency shutdown),
- The alarm system.

The purpose of an alarm system is to bring a malfunction to the attention of the operator, whereas a trip system takes protective or corrective action when a fault condition occurs. A trip system could shutdown the process in an orderly manner, or switch over from some defective unit to a standby unit.

Thus, an alarm system is not another interlock or protection system.

An alarm system forms an essential part of the operator interface to the plant system. It provides essential support to the operator by warning him of situations that need his attention. Hence it has an important role in preventing, controlling and mitigating the effects of abnormal situations.

2.1 Purpose of the alarm management

The fundamental purpose of alarm annunciation (presentation to the operator) is to alert the operator to deviations from normal operating conditions, i.e. abnormal operating situations. The ultimate objective is to prevent, or at least minimise, physical and economic loss by triggering operator intervention in response to the alarm. A key factor in operator response effectiveness is the speed and accuracy with which the operator can identify the alarms that require immediate action.

Alarm management is the application of human factors (or ergonomics) along with instrumentation engineering to design an alarm system and to increase its usability and then its efficiency. Most often the major usability problem is that there are too many alarms presented during a plant system upset, commonly referred to as alarm flood.

With modern technology and industrial control system such as EPICS, alarms are easy and cheap to configure and deploy, resulting in a combination of too much data collided with too little useful information.

In addition, a poorly designed alarm system comes with many problems such as improperly set alarm points, ineffective annunciation, unclear alarm messages, alarms standing for long periods (days or weeks), etc.

Good alarm management helps the operator to maintain the plant system within a safe operating envelope and to correct potentially dangerous and costly situations before the emergency shutdown system is forced to intervene. Thus good alarm management improves the plant system availability.
2.2 Indicators of poor alarm management

The main problems in alarm management are nuisance alarms, stale alarms, alarm floods and lack of clarity of the alarm to the operator.

2.2.1 Nuisance Alarms

Nuisance alarms are alarms that indicate an abnormal condition when none exists, when no change in process condition has occurred or when alarm condition comes and goes on a regular basis or intermittently. Nuisance alarms desensitise the operator, reducing the response to all alarms, even those requiring immediate action.

Instrument problems, maintenance issues or alarm levels set within the normal operating range often cause nuisance alarms. During operation, analysis of the alarm frequency by alarm identifier is used to detect nuisance alarms. Once detected, nuisance alarms should be investigated and corrected. Typical alarm reports show a very small percentage is responsible for the majority of alarms. Without monitoring and prompt follow-up, nuisance alarms can quickly deteriorate the performance of an alarm system.

2.2.2 Stale or Standing Alarms

Stale or standing alarms are alarms that remain in the alarm state for extended periods when no abnormal condition exists or no operator action is required. Stale alarms form a baseline of alarms that require no action and train the operator to ignore certain alarms. These alarms are often caused by alarm configuration problems, un-cleared alarms after operator action has been taken or alarm levels set within the steady-state conditions. Measurement of the alarm standing time is used to detect stale alarms. Without monitoring and follow-up, the number of stale alarms slowly increases, decreasing the effectiveness of the alarm system.

2.2.3 Alarm Floods

Alarm floods are a temporary high rate of alarms, usually associated with an event like a process upset. Alarm floods overwhelm the operator, masking the important alarms and reducing the operator's ability to correctly respond to the abnormal situation. Alarm floods are often caused by configuring multiple or cascading alarms for a given event. Alarm floods are detected by measuring the rate of alarms in a given time interval. Alarm floods are one of the more difficult problems to solve, but a problem closely linked with plant disasters. Monitoring can detect and report alarm floods, but reducing floods requires detailed process understanding and good alarm practices, particularly alarm rationalisation.

2.2.4 Alarm Clarity

Clarity of alarms is an issue related both to configuring the alarms and to training the operator to respond to the alarm. Alarm documentation generated during rationalisation provides the information for training. Alarm clarity problems are a difficult thing to measure but operator training can provide the opportunity to identify clarity problems ensuring that alarm message provides meaningful information to the operator concerning the cause of the problem or the corrective action.

2.3 What is an Alarm?

A fundamental part of alarm management is the definition of an alarm: an audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a response. One essential element of this definition is the response to the alarm.
2.4 Alarm management lifecycle

The alarm management lifecycle covers the design and maintenance activities from philosophy to management of change, thus from initial conception through decommissioning. The figure below shows the essential steps and identifies the alarm philosophy as the entry point of the alarm management.

![Alarm Management Lifecycle Diagram]

2.4.1 Philosophy

The alarm philosophy documents the ITER approach to alarm management. It includes the definitions and principles for the alarm system as well as the details of the practices and procedures for each of the remaining life cycle stages.
2.4.2 Identification

Identification of possible alarms can be done by many methods, such as a process hazard analysis, risk assessment or incident investigations. At this stage the need for an alarm has been identified and it is ready to be rationalised.

2.4.3 Rationalisation

Rationalisation is the process of reconciling each individual alarm against the principles and requirements of the alarm philosophy and generating supporting documentation such as operator action, response time, and consequence of deviation description. This information is critical to improving alarm clarity for the operator.

Once the consequences and the allowable response time have been documented, a priority is assigned to the alarm.

At this stage the alarm requirements regarding design, testing, training and reporting are also captured. The outputs of this stage are the alarm database and alarm design requirements.

2.4.4 Detailed Design

The design stage includes the basic configuration of alarm attributes. Many nuisance alarms and stale alarms can be eliminated with good basic configuration practices.

The HMI design includes display and annunciation for the alarm, text message for operator guidance and optionally links to a detailed synoptic of the plant area concerned or external documentation. The output of this phase is the completed alarm design.

2.4.5 Implementation

Implementation is the stage where the design is put into service. This process includes training for the operator and initial testing. This process is one step in addressing alarm clarity.

2.4.6 Operation

Operation is the life cycle stage when the alarm is in service and reporting abnormal conditions to the operator. The outputs of this stage are the operational alarms list and alarm response procedures.

2.4.7 Maintenance

In the maintenance stage, the alarm or alarm system is not operational but is being tested or repaired.

2.4.8 Monitoring and Assessment

Performance monitoring is the periodic collection and analysis of data from alarms in the operation life cycle stage. Without monitoring, it is almost impossible to maintain an effective alarm system. It is the primary method to detect problems such as nuisance alarms, stale alarms, and alarm floods. The assessment may trigger maintenance work or identify the need of changes based on the alarm monitoring report.

2.4.9 Management of Change

Management of change is the structured process of approval and authorisation to make additions, modifications, and deletions of alarms from the system. Requirements for changes may be identified by many means, including operator suggestions and monitoring. The change process should feed back to the identification stage to ensure that each change is consistent with the alarm philosophy. The outputs of this phase are the authorised alarm changes.

2.4.10 Audit

Periodic reviews are conducted to maintain the integrity of the alarm system and its associated processes. Alarm philosophy could be adapted as a result of an audit in order to improve the alarm system. The outputs of this stage are recommendations for improvement.
## 2.5 Alarm Glossary

This appendix provides a glossary of some of the terms used in ITER Alarm Handler System. It is not intended to be comprehensive, but to concentrate on those terms that are likely to be unclear or cause confusion.

<table>
<thead>
<tr>
<th>Definitions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abnormal situation</td>
<td>A disturbance of series of disturbances in a process that cause plant operations to deviate from their normal operating state.</td>
</tr>
<tr>
<td>Acknowledged/Unacknowledged</td>
<td>Alarm state: an alarm is acknowledged when the operator has indicated awareness of its presence. It is unacknowledged until this has been done.</td>
</tr>
<tr>
<td>Active alarm</td>
<td>An alarm condition which is on (i.e. limit has been exceeded and condition continues to exist).</td>
</tr>
<tr>
<td>Alarm</td>
<td>An audible or visual means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a response.</td>
</tr>
<tr>
<td>Alarm deadband</td>
<td>When a deadband is applied, then the alarm is raised at one level but cleared at a different level.</td>
</tr>
<tr>
<td>Alarm flood alarm overload</td>
<td>The situation where more alarms are received that can be effectively addressed by a single console operator - e.g. in steady state, more than 1 alarm per 10 minutes; more than 10 alarms during the first 10 minutes of a major plant upset.</td>
</tr>
<tr>
<td>Alarm limit alarm threshold</td>
<td>The threshold value or discrete state of a process variable that triggers the alarm.</td>
</tr>
<tr>
<td>Alarm management</td>
<td>The processes and practices for determining, documentation, designing, operating, monitoring and maintaining alarm handler systems.</td>
</tr>
<tr>
<td>Alarm priority</td>
<td>The ranking of alarms by severity and response time (e.g. seriousness of consequences and allowable response time).</td>
</tr>
<tr>
<td>Alarm system Alarm Handler System</td>
<td>The collection of hardware and software that detects an alarm state, transmits the indication of that state to the operator, and records changes in the alarm state.</td>
</tr>
<tr>
<td>Alert</td>
<td>A lower priority notification that an alarm, that has no serious consequence if ignored or missed.</td>
</tr>
<tr>
<td>Chattering alarm</td>
<td>An alarm that repeatedly transitions between the alarm state and the normal state in a short period of time.</td>
</tr>
<tr>
<td>Cleared</td>
<td>Alarm state: an alarm is cleared when the condition has returned to normal.</td>
</tr>
<tr>
<td>Critical alarm</td>
<td>The highest level of alarm priorities – immediate operator action is required or a serious plant incident will occur.</td>
</tr>
<tr>
<td>Latching alarm</td>
<td>An alarm that remains in alarm state after the process has returned to normal and requires an operator reset before it will clear.</td>
</tr>
<tr>
<td>Nuisance alarm</td>
<td>An alarm that annunciates excessively, unnecessarily, or does not return to normal after the correct response is taken (e.g. chattering, fleeting or stale alarm).</td>
</tr>
<tr>
<td>Operator response time</td>
<td>The time between the annunciation of the alarm and when action is required to prevent the consequences of the alarm related event.</td>
</tr>
<tr>
<td>Priorisation</td>
<td>The process of assigning to an alarm a level of operational importance.</td>
</tr>
<tr>
<td>Raised</td>
<td>An alarm is raised or initiated when the condition creating the alarm is occurred.</td>
</tr>
<tr>
<td>Reset</td>
<td>An alarm is reset when it is in a state that it can be removed from the displayed list (cleared and acknowledged).</td>
</tr>
<tr>
<td>Masking shelving</td>
<td>Masking is a facility where the operator is able to temporarily prevent an alarm from being displayed to him when it is causing nuisance. A masked alarm will be removed from the list and will not re-annunciate until unmasked.</td>
</tr>
<tr>
<td>Stale alarm</td>
<td>An alarm that remains in the alarm state for an extended period of time (e.g. 24 hours).</td>
</tr>
<tr>
<td>Suppress</td>
<td>An alarm is suppressed when logical criteria are applied to determine that the alarm should not occur, even though the base alarm condition (e.g. alarm setting exceeded) is present.</td>
</tr>
</tbody>
</table>
3 Alarm philosophy principles

* The core principles of this alarm philosophy [RD1] are the following:

- **Usability**: the alarm system should be designed to meet user needs and operate within ergonomic requirements. This means that the support information alarm should:
  - Be relevant to the user's role at the time,
  - Indicate clearly what response is required,
  - Be presented at a rate that the user can deal with particularly when the plant system is upset or in an unusual condition,
  - Be easy to understand.

- **Performance monitoring**: the performance of the alarm system should be assessed during design and commissioning to ensure that it is usable and effective under all operating conditions. Regular auditing should be continued throughout the plant system life to confirm that good performance is maintained.

- **Engineering**: the design should follow structured methodology in which every alarm should be justified, documented and properly engineered. This initial investment in the design should be sufficient to avoid the operational problems which result at the end in overall higher lifetime costs.

3.1 What is an Alarm System?

Alarm System refers to the complete system – hardware and software items - for generating and handling alarms including signal conditioning and transmission, alarm processing and alarm display. It also includes supporting information such as operator guidance and documentation.

The function of an alarm system is to alert operators to plant conditions, such as deviation from normal operating limits and to abnormal events, which require timely action or assessment.

3.2 The role of the operator

The role of an operator on ITER encompasses a range of different activities including plant operation, fault identification, co-ordination of maintenance… The tasks involved change depending on plant state, e.g. whether it is in normal operation or start up, upset operation, emergency shutdown or planned shutdown.

The control system automatically acts to mitigate disturbances to keep the plant close to target operating conditions. Significant disturbances may put the plant into an upset state from which the control system cannot recover without operator intervention. Alarms should be provided to present this need for operator intervention/action.

If the upset state is not corrected in time by the operator and the plant condition approaches a state where damage is likely to occur, the emergency shutdown (ESD) is started. Figure 3.2 illustrates the process conditions from normal and target conditions to abnormal conditions of upset and shutdown.

![Figure 3.2 – Process condition model](image-url)
3.3 **Characteristics of a good Alarm System**

Some of the characteristics of ITER Alarm System are summarised in Table 1:

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Relevant</th>
<th>Unique</th>
<th>Timely</th>
<th>Prioritised</th>
<th>Understandable</th>
<th>Diagnostic</th>
<th>Advisory</th>
<th>Focusing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Not spurious or of low operational value</td>
<td>Not duplicating another alarm</td>
<td>Not long before any response is needed or too late to do anything</td>
<td>Indicating the importance that the operator deals with the problem</td>
<td>Having a message which is clear and easy to understand</td>
<td>Identifying the problem that has occurred</td>
<td>Indicative of the action to be taken</td>
<td>Drawing attention to the most important issues</td>
</tr>
</tbody>
</table>

Table 2.3 – Characteristics of ITER Alarm System

3.4 **Key Design Principles**

* The purpose of ITER alarm system is to direct the operator’s attention towards plant conditions requiring timely assessment or action. To achieve this goal, each alarm should be designed carefully according key principles:

- Each alarm should alert, inform and guide,
- Every alarm presented to the operator should be useful and relevant to the operator,
- Each alarm must have a defined operator action or response,
- The consequence if the alarm is not treated properly by the operator should be explicit,
- Adequate time should be allowed for the operator to carry out a defined response,
- Each alarm must be rationalised prior to installation,
- Each alarm will be designed in accordance with given guidelines,
- Operator training is required for each alarm prior to installation,
- Alarm system performance must be monitored on a daily basis and corrective action taken when performance limits are not met,
- All additions, modifications, and deletions of alarms must follow a ”management of change” procedure.

3.5 **Context sensitive**

The alarm system needs to be “context sensitive” and take account of the current operational state when determining which signals should trigger alarms. Some process variables that would trigger alarms in normal operation may not be relevant during a start up or maintenance phase. For instance, it is required that all ICH electronic tube cathode heaters and control grids are biased and switched off between shots to reduce the stress and fatigue on internal components due to anode voltage biasing. That means that the correct status of these ICH components depend of the Plasma Operation State.

Alarm context sensitive implies logical processing to control the triggering of alarms to respond to changes in the mode of operation or the operating conditions.
3.6 **Alarm for redundant components**

Redundant components such as pumps or valves require special care in the alarm identification process. The alarm should not be associated with each individual component failure state but more on the number of necessary running components for operation.

In addition redundant measurements can generate multiple alarms all indicating the same problem. Suppression logic should be implemented to ensure that only a single alarm is displayed to the operator.

3.7 **Dependant failures**

It is important to carefully assess dependant failures sometimes referred to as common cause or common mode of failure. This is the case when sharing measurements, process or services such as power supplies or network.

3.8 **Alarm Engineering Checklist**

One way to formalise the alarm identification and design process is to use a checklist to justify and document each alarm:

- What is the purpose of this alarm?
- What hazard or process risk is this alarm intended to provide warning of?
- What should the operator do in response to this alarm?
- What happens if no action is taken by the operator to this alarm?
- How much time is there to react to this alarm?
- How likely is it that the operator response will be effective? If the operator cannot do anything to prevent the risk indicated by the alarm, then it is providing little benefit and should not be an alarm.
- How frequently is the risk likely to occur? Once a week? Once a month? Several times a year? Once a year, 3 years, 5 years, 10 years?
- Is a protective system against the risk used as well as the alarm system?
- What is the severity of the risk in terms of potential plant damage, economic loss and plant availability?
- Should the alarm priority be automatically changed according to operating conditions: shutdown, starting up, plasma operation, maintenance mode?
- Is the alarm context sensitive? Does the alarm setting need to change according to operating conditions?
- How much does the process variable that triggers the alarm fluctuate in normal operation?
- What deadband would be suitable?
- What are the conditions to clear and suppress the alarm?
- Is the alarm associated with a shared measurement, services or process?
- Will the alarm require testing and how will it be tested?
4 Rationalisation

Rationalisation is the process of examining one alarm at a time against the principles defined in the alarm philosophy. The product of rationalisation is a set of consistent, well-documented alarms. The documentation supports both the design process and operator training.

Rationalisation begins with identifying the process variable, the rationale for the alarm and the associated action. If the alarm is consistent with the philosophy, it is prioritised based on consequences and response time. Any further requirements for the alarm design are captured as well.

The basic control system information regarding an alarm includes:

- Process variable identification that triggers the alarm,
- Alarm type,
- Description,
- Units/states,
- Setting/alarm state.

The process variable identification is the identification of the PV in EPICS database that triggers the alarm. The alarm type describes the alarm as a Limit Alarm – high-high, high, low, low-low, or a State Alarm. The description is also taken from the EPICS database [maximum 40 characters]. The units are the engineering units for an analogue type value, and the states are the discrete values of a digital value. The setting is the analogue alarm limit or the discrete state that triggers the alarm.

Some information is required to train the operator to respond to the alarm:

- Consequence of deviation,
- Corrective action,
- Time for response,
- Consequence category,
- Basis.

Other information is required to complete the requirement specifications:

- Priority,
- Notification requirements.

The priority in the operator interface is a critical way to designate the importance of the alarm. Depending on how the alarm affects the plant and how much time is there to react, the priority should be defined using the alarm severity field in EPICS database. This could be:

- MINOR: moderately out of tolerance and enough response time,
- MAJOR: significantly out of tolerance or a fault and/or time critical (response time within 3 minutes),
- Invalid: invalid data or no communication - this is the highest severity condition.

The alarm may be set up to be annunciated, or simply displayed on the operator console in the active alarm view.
Example of alarms rationalisation with 2 process variables generating low-low and high-high limit alarms:

<table>
<thead>
<tr>
<th>Alarm 1</th>
<th>Alarm 2</th>
<th>Alarm 3</th>
<th>Alarm 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>PV</td>
<td>LIG502</td>
<td>LIG502</td>
<td>PIG502</td>
</tr>
<tr>
<td>Alarm type</td>
<td>LOLO</td>
<td>HIHI</td>
<td>LOLO</td>
</tr>
<tr>
<td>Description</td>
<td>T502 Level</td>
<td>T502 Level</td>
<td>T502 Pressure</td>
</tr>
<tr>
<td>Units/states</td>
<td>%</td>
<td>%</td>
<td>INWC</td>
</tr>
<tr>
<td>Setting/alarm state</td>
<td>10</td>
<td>90</td>
<td>1</td>
</tr>
<tr>
<td>Consequence of deviation</td>
<td>Cavitate pump</td>
<td>Overflow tank</td>
<td>Air intrusion</td>
</tr>
<tr>
<td>Corrective action</td>
<td>Stop pump</td>
<td>Close inlet valve</td>
<td>Stop pump</td>
</tr>
<tr>
<td>Response time</td>
<td>10 min</td>
<td>2 min</td>
<td>10 min</td>
</tr>
<tr>
<td>Consequence category</td>
<td>Equipment</td>
<td>Safety</td>
<td>Safety</td>
</tr>
<tr>
<td>Basis</td>
<td>Pump cavitation at 2%</td>
<td>Tank overflow at 107%</td>
<td>Vacuum breaker setting</td>
</tr>
<tr>
<td>Priority</td>
<td>MINOR</td>
<td>MAJOR</td>
<td>MAJOR</td>
</tr>
<tr>
<td>Notification requirements</td>
<td>Alarm view</td>
<td>Alarm view</td>
<td>Alarm view</td>
</tr>
</tbody>
</table>

5 Detailed Design

EPICS records generate alarms. The types of alarms fall into the following categories: scan alarms, read/write alarms, limit alarms, and state alarms. Some of these alarms can be configured [limit alarms, and state alarms], and some are automatically managed by the device support [scan alarms, read/write alarms – alarm severity is always set to INVALID for invalid data or no communication].

5.1 Limit Alarm

Alarm limits can be configured for analogue records (Analog Input [AI], Analog Output [AO], Calculated PV [CALC]… records). There are two limits for above normal operating range – high-high [HIHI] and high [HIGH] and two limits for the below-limit operating range – low-low [LOLO] and low [LOW] so that a warning can be set off before the value goes into a dangerous condition.

Each of these limits may have an associated alarm severity: MAJOR, MINOR, NO_ALARM or INVALID. If the record's value drops below the low limit and an alarm severity of MAJOR was specified for that low limit, then a MAJOR alarm is triggered. When the severity of a limit is set to NO_ALARM, none will be generated.

Analogue records also contain a hysteresis field, which is used when determining limit violations. The hysteresis field is the deadband around the alarm limits. The deadband keeps a signal that is hovering at the limit from generating too many alarms.
In this example the range is -100 to 100 Volts [LOPR] – [HOPR], the high alarm limit is 30 Volts [HIGH], and the hysteresis is 10 Volts [HYST]. If the value is normal and approaches the HIGH alarm limit, a MAJOR alarm is generated when the value reaches 30 Volts. This will only go to normal if the value drops below the limit by more than the hysteresis. For instance, if the value changes from 30 to 28 this record will remain in HIGH alarm. Only when the value drops to 20 will this record return to normal state.

EPICS representation in the database file will be:

```plaintext
record(ai, "TIG503")
{
    field(DESC, "Power Supply")
    field(EGU, "Volts")
    field(LOPR, "-100")
    field(HOPR, "100")
    field(HIGH, "30")
    field(HSV, "MAJOR")
    field(HYST, "10")
}
```

Simply enabling all possible alarms on an EPICS record will often result in a flow of useless alarms: 4 alarms could be triggered by each analogue record just by specifying for each threshold (HIHI, HIGH, LOW, LOLO) a severity (HHSV, HSV, LSV, LLSV). But, will the HIHI alarm require a significantly different operator response from the HIGH alarm? Will there be sufficient time to react between these 2 alarms, or will each HIGH alarm be followed by a HIHI alarm anyway?

As discussed previously, the thresholds should generally be set according to operational conditions and not be fixed numbers. This required additional EPICS database logic such as CALC record to dynamically compute the limits and AO records to write them to the threshold fields.

In this example, HIGH alarm limit in TIG503 AI record is set by an AO record which gets its output value (DOL field) from a CALC record which calculates the limit according to the current operational state.

In addition to activate alarms in the operating states for which they are relevant, it could be necessary to change alarm priority MINOR/MAJOR based on the current operating state. This will also be done by adding EPICS database logic.

Finally, in some cases, the actual limits check is performed inside a PLC, FPGA or any black box. This means that the analogue PV is separate from the alarm trigger usually represented by a binary independent PV.
5.2 State Alarm

State alarms could be configured for discrete values (Binary Input [BI], Binary Output [BO], Multi-Bit Binary Input [MBBI], Multi-Bit Binary Output [MBBO]...). In this case, a certain state can trigger an alarm.

Consider a cooling fan whose discrete states are High, Low, and Off. The Off state can be configured to be an alarm condition so that whenever the fan is off the record is in a state alarm. The severity of this error is configured for each state. In this example, the Low state could be a state alarm of MINOR severity, and the Off state a state alarm of MAJOR severity.

EPICS representation in the database file will be:

```plaintext
record(mbbi, "CF917")
{
    field(DSC, "Cooling Fan")
    field(ZRVL, "0")
    field(ZRST, "Off")
    field(ZRSV, "MAJOR")
    field(ONVL, "1")
    field(ONST, "Low")
    field(ONSV, "MINOR")
    field(TWVL, "2")
    field(TWST, "High")
    field(TWSV, "NO_ALARM")
}
```

Discrete records also have a specific field (UNSV) used to specify the severity of an unknown state to NO_ALARM, MINOR or MAJOR. If set, the unknown state severity field triggers an alarm when the record support routine cannot find a matching value in the state value fields for VAL or when VAL is out of range.

The change of state severity field (COSV) triggers an alarm when the record's state changes, if set to MAJOR or MINOR. Thus, the operator can be informed when the record's alarm state has changed. If this field specifies NO_ALARM, then a change of state will not trigger a change of state alarm. If specified either MINOR or MAJOR, a change of state will trigger an alarm with the corresponding severity.

As explained in previous section, the alarm condition is often contextual and requires additional condition-based logic implemented by CALC records in order to trigger useful alarms.

5.3 Alarm HMI

5.3.1 Alarm information in mimics

It is often useful to enable for instance all analogue alarm limits (HIHI, HIGH, LOW, LOLO) for HMI animation purposes, allowing a graphical widget such as a gauge, meter, tank or thermometer to display red (MAJOR alarm), brown (MINOR alarm) or magenta (invalid alarm) borders around the normal operating conditions.

This type of alarms is separate from the process alarm trigger record which is contextual and requires additional logic. While the latter requires careful rationalisation and design, alarms for HMI purposes follow a lighter process but need to be part of the operator documentation and training.
5.3.2 Alarm Related Display

In order to help the operator to manage an alarm, a related display could be defined as a link to detailed equipment documentation or maintenance procedure or a specific mimic with test and diagnostic commands.

5.3.3 Alarm Tree View

The process alarms are organised in a hierarchical manner. The operator can browse the alarm configuration components and their related alarm status in a tree-like structure, which by default includes all configured alarms, active or not.

Usually, alarm limits for HMI animation are excluded from the alarm tree configuration in order to avoid unnecessary cluttering.

5.3.4 Active Alarm View

The Active Alarms View provides a tabular view of currently active alarms. It shows alarms that actually triggered and not yet cleared.

5.3.5 Acknowledged Alarm View

Alarm acceptance by the operator is available on both views – alarm tree and active alarm – and applies to an individual or group of alarms.

The Acknowledged Alarms View provides the list of alarms acknowledged by the operator as soon as they are suppressed from the active alarm view.

5.3.6 Message History

The Message History includes events from the alarm system such as:

- A new alarm triggered,
- The state of an alarm changed,
- Operator acknowledged/un-acknowledged an alarm,
- Alarm system related operation, for instance an alarm configuration change.

6 Implementation

6.1 Alarm Testing

Testing is a common requirement when the design is implemented. Testing requirements vary with the type of alarms. Initial and periodic testing requirements should be documented in the rationalisation so accommodation for testing can be made in the design step.

6.2 Training

Training is an essential step in developing an alarm system. Since an alarm exists only to notify the operator to take an action, the operator must know the corresponding action for each alarm, as defined in the alarm rationalisation.

Documentation on all alarms should be easily accessible to the operator in a standard way:

- Purpose of the alarm,
- Alarm conditions,
- Operator guidance,
- Failure consequence,
- Operator response time available,
- Contacts,
- Additional information.
7 Monitoring and assessment

Monitoring alarm systems is a critical step in alarm management. Since each alarm requires operator action for success, overloading the operator reduces the effectiveness of the alarm system. Instrument problems, controller performance issues and changing operating conditions will cause the performance of the alarm system to degrade over time. Monitoring and taking action to address bad actors can maintain a system at the desired level of performance.

A first indicator is the number of installed alarms per operator:\footnote{This indicator is defined per operator and it should be clarified if an operator deals with one or many plant systems.}

\textit{Fewer than 100 configured alarms is recommended.}

Then, the average alarm rates provide a good and simple indication of the workload imposed on the operator by the alarm system.

In steady operation:

- More than 1 alarm per minute is \textit{unacceptable} as the operator need some time to carry out the expected action,
- 1 alarm per 2 minutes is considered \textit{over-demanding},
- 1 alarm per 5 minutes is \textit{manageable}.

* \textit{In steady operation, less than 1 per 10 minutes is recommended.}

* \textit{The number of alarms during the first 10 minutes of a major plant upset should be less than ten.}

* \textit{The recommended alarm priority distribution is MAJOR (20 percent) and MINOR (80 percent).}

* \textit{The average number of standing alarms should be less than ten.}

To support the alarm philosophy, measurement tools will report on different metrics:

- Frequency of alarms, such as total number of alarms per day,
- Frequency of triggered alarms, such as the number of times per day an alarm has been triggered,
- Duration of standing alarms - the number of minutes a triggered alarm is active,
- Rate of alarms, such as number of alarms per ten-minute interval,
- The number of alarm floods (more than 10 alarms per 10 minutes) per day.