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>
<th>Name</th>
<th>Action</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author</td>
<td>Utzel N.</td>
<td>21 Aug 2017:signed</td>
<td>IO/DG/COO/SCOD/CSD/CDC</td>
</tr>
<tr>
<td>Co-Authors</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reviewers</td>
<td>Park M.</td>
<td>04 Sep 2017:recommended</td>
<td>IO/DG/COO/SCOD/CSD/CDC</td>
</tr>
<tr>
<td></td>
<td>Petitpas P.</td>
<td>04 Sep 2017:recommended</td>
<td>IO/DG/COO/SCOD/CSD/PCI</td>
</tr>
<tr>
<td>Approver</td>
<td>Wallander A.</td>
<td>04 Sep 2017:approved</td>
<td>IO/DG/COO/SCOD/CSD</td>
</tr>
</tbody>
</table>

#SecureIDM#

RO: Park Mikyung

Read Access
LG: CODAC team, AD: ITER, AD: External Collaborators, AD: IO_Director-General, AD: EMAB, AD: OBS - CODAC Section (CDC), AD: Auditors, AD: ITER Management Assessor, project administrator, RO, AD: OBS - Control System Division (CSD) - EXT, AD: OBS - CODAC Section (CDC) - EXT, LG: Cryogenic Section lin...
## Change Log

**Philosophy of ITER Alarm System Management (3WCD7T)**

<table>
<thead>
<tr>
<th>Version</th>
<th>Latest Status</th>
<th>Issue Date</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1.0</td>
<td>Approved</td>
<td>02 Dec 2010</td>
<td></td>
</tr>
<tr>
<td>v1.1</td>
<td>Signed</td>
<td>05 Jan 2011</td>
<td>Internal Review Comments integrated.</td>
</tr>
<tr>
<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>v2.1</td>
<td>Approved</td>
<td>01 Feb 2013</td>
<td>PCDH V7 schema</td>
</tr>
<tr>
<td>v2.2</td>
<td>Approved</td>
<td>21 Aug 2017</td>
<td>Redundant parts with &quot;[RD5] ITER process for Alarm System Development (ITER_D_3UZXA2 v1.1)&quot; have been removed. New reference to &quot;[RD6] D2.2 ITER Alarm System Management (RKSTSP v1.0)&quot;. New Alarm Operator Interface based on &quot;ITER Human Factors requirements for HMI development (QEDG6L)&quot;.</td>
</tr>
</tbody>
</table>
# Table of Contents

1 Introduction .......................................................................................................................... 2  
  1.1 PCDH Context .................................................................................................................. 2  
  1.2 Document Scope ............................................................................................................ 2  
  1.3 Alarm Glossary ............................................................................................................. 3  
  1.4 Related Documents ...................................................................................................... 4  

2 Alarm Philosophy Principles .............................................................................................. 5  
  2.1 The Role Of The Operator ............................................................................................. 5  
  2.2 What Is An Alarm? ......................................................................................................... 6  
  2.3 What Is An Alarm System? ........................................................................................... 6  
  2.4 Characteristics Of A Good Alarm System .................................................................... 6  
  2.5 Indicators Of Poor Alarm System ................................................................................. 7  
    2.5.1 Nuisance Alarms .................................................................................................... 7  
    2.5.2 Stale Or Standing Alarms ...................................................................................... 7  
    2.5.3 Alarm Floods ........................................................................................................ 7  
    2.5.4 Alarm Clarity ........................................................................................................ 7  
  2.6 Key Design Principles .................................................................................................. 8  
  2.7 Context Sensitive ......................................................................................................... 8  
  2.8 Alarm For Redundant Components ............................................................................. 8  
  2.9 Dependant Failures ...................................................................................................... 8  
  2.10 Alarm Engineering Checklist ..................................................................................... 9  

3 Detailed Alarm Design ...................................................................................................... 10  
  3.1 Limit Alarm .................................................................................................................. 10  
  3.2 State Alarm .................................................................................................................. 11  
  3.3 Alarm Configuration .................................................................................................... 11  
    3.3.1 Alarm enabled ...................................................................................................... 11  
    3.3.2 Alarm latched ...................................................................................................... 12  
    3.3.3 Alarm annunciated ............................................................................................ 12  
    3.3.4 Alarm suppression .............................................................................................. 12  
    3.3.5 Alarm Guidance ................................................................................................. 12  
    3.3.6 Alarm Page ........................................................................................................ 13  
    3.3.7 Commands And Automated Actions ................................................................... 13  

4 Alarm Operator Interface ................................................................................................ 14  
  4.1 Alarm States ................................................................................................................ 14  
  4.2 Alarm Pane .................................................................................................................. 14  
  4.3 Alarms List .................................................................................................................. 15  
  4.4 Alarm Coding ............................................................................................................. 16  
  4.5 Message History ......................................................................................................... 17
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)

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 Alarm Glossary

<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 alarm hysteresis</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 operator terminal.</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 [RD5].</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) [RD6].</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>
1.4 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)
[RD6] D2.2 ITER Alarm System Management (RKSTSP v1.0)
2 Alarm Philosophy Principles

The core principles of the alarm philosophy 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. According to the routing principle [RD6] alarms shall be routed only to operator(s) or person(s) required to respond to the alarm,
  - Be prioritised. The purpose of prioritising alarms [RD6] is to support an operator make decisions about what aspect of the plant needs most attention when a number of alarms occur together,
  - 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 [RD5] 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.

2.1 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 and service interruption is likely to occur, the emergency shutdown (ESD) is started.

Figure 2-1 illustrates the process conditions from normal and target conditions to abnormal conditions of upset and shutdown and shows the operator intervention within normal conditions.
### 2.2 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.

Alarms should be used at the point that operator action is necessary and should be treated differently from “warnings” and other plant information.

### 2.3 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.

### 2.4 Characteristics Of A Good Alarm System

Some of the characteristics of ITER Alarm System are summarised in Figure 2-2:

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

Figure 2-2 Characteristics of ITER Alarm System
2.5 Indicators Of Poor Alarm System

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

2.5.1 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.

2.5.2 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.

2.5.3 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.

2.5.4 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.
2.6 **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.

2.7 **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, during and between pulses 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. As a consequence the on/off position signals of these ICH components cannot trigger alarms as the alarm status depends on the operational state and position.

The processing logic to control the triggering of alarms can be implemented on the controller or using EPICS soft process variables on the PSH.

2.8 **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 based on the number of necessary running components for operation.

2.9 **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.

Suppression logic should be implemented to ensure that only a single alarm is displayed to the operator.
2.10 **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?
3 Detailed Alarm Design

Alarms are generated by EPICS records. The types of alarms fall into the following categories:

- Alarms automatically managed by the device support - scan failure alarms and read/write failure alarms: the alarm severity is always set to INVALID to indicate invalid data and communication issue,
- Configurable alarms based on limits and states.

3.1 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 HYST, 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")
}
```

A low-pass filter AFTC field can also be used to specify a delay for reporting alarms caused by the input level passing the HIGH, HIHI, LOW or LOLO values.
3.2 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 given state can trigger an alarm.

Consider the following example of 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.

Discrete records also have a specific field UNSV used to specify the severity of an unknown state to usually INVALID. 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 can trigger an alarm when the record's state changes, 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.

3.3 Alarm Configuration

During the design phase, CODAC provides tools to edit each CBS alarm configuration:

- EPICS records and alarm fields - alarm limits and states, alarm severities and hysteresis
- Alarm suppression logical criteria
- Alarm response
- Automatic actions such as sending an email or creating an electronic logbook entry.

3.3.1 Alarm enabled

It is often useful to enable analogue alarm limits HIHI, HIGH, LOW, LOLO for HMI animation purposes, allowing a graphical scaled widget such as a gauge, meter, tank or thermometer to show what is the current value compared to the normal operating limits.

For redundant components, it is important to indicate on the HMI when one of them is in failure state even though it does not trigger an alarm as the redundant equipment took over. This is done by setting the alarm fields of each component state record.
Similarly, dependant failures have to be shown on HMI but only the root cause of the problem shall be defined as an alarm.

So, EPICS alarm fields can be set on any record but only when the variable is configured as “alarm enabled” will it be considered as an ITER alarm vs. alarm for display only. By default alarms are not enabled.

### 3.3.2 Alarm latched

By default ITER alarms are configured to be latched i.e. they remain in alarm state after the process has returned to normal and requires an operator acknowledgment before being removed from the alarms list.

### 3.3.3 Alarm annunciated

Optionally, an alarm can be configured to be annunciated. In this case, the alarm description prefixed by the alarm severity is converted to speech, but it is also possible to customise the annunciated message.

For example, a MAJOR alarm on a process variable with description "Low Water Pressure" will result in the following default annunciation:

```
MAJOR alarm: Low Water Pressure
```

*Note: a sound card and speakers on the operator terminal are required for alarm annunciation.*

### 3.3.4 Alarm suppression

In addition to the low-pass filter \texttt{AFTC} EPICS field, it is possible to add a delay (in seconds) on the alarm system to take into account a new alarm only after its alarm severity remains for at least this time.

When an additional alarm count greater than zero is specified, the alarm system will react to alarms that either outlast the delay, or happen at least "count" times within the delay.

Both these options can reduce the amount of nuisance alarms from noisy process variables, but in practice it is always best to cure the problem at the source through adequate dead-bands or smoothing.

A filter expression can be used to enable or disable alarms automatically. The filter expression can be something like:

```
some\_other\_pv > 5
```

to only enable the alarm when the other PV has a value above 5.

Ideally, context sensitive alarms are handled on the controller or the PSH by adding logic that prevents the alarm from being generated, instead of generating an alarm but then disabling it in the alarm server.

*Limitation: the alarm server subscribes to alarm state changes and not variable changes. An alarm expression like \texttt{some\_other\_pv > 5} will not be evaluated for each change in the value of \texttt{some\_other\_pv}; it will only be evaluated for changes in the alarm state of \texttt{some\_other\_pv}, so the value changes used in the filter expression must also be alarm state changes of \texttt{some\_other\_pv} – i.e. HIGH value 5 shall trigger a MINOR alarm on \texttt{some\_other\_pv} for instance.*

### 3.3.5 Alarm Guidance

Alarm guidance configuration provides a quick access to alarm information via a right-click on the alarm message. It is a good practice to insert here:

- Purpose of the alarm,
- Alarm conditions,
- Operator guidance,
- Failure consequence,
- Operator response time available,
- Contacts,
- Additional information and links.
3.3.6 Alarm Page

For each enabled alarm, it is required to provide an alarm page (also called related display) which details the procedure that the operator has to follow in order to take a corrective action.

The automatically generated template contains information provided for the alarm guidance but has to be completed. Figure 3-1 provides an illustration of an UTIL-S15 alarm page.

![Figure 3-1 UTIL-S15 TECSystem Fault alarm page](image)

3.3.7 Commands And Automated Actions

It is possible to specify for an alarm a list of commands that the operator might want to invoke manually via a right-click on the alarm message.

Another option is to define for an alarm automated actions executed if the alarm persists for a certain time without being acknowledged or cleared. An automated action can be sending an email, creating an electronic logbook entry and executing a command.

*Note: automatic emails require the configuration of the SMTP host server and mail sender.*
4 Alarm Operator Interface

4.1 Alarm States

The following alarm states are used consistently across all displays:

- Acknowledged – when the operator has indicated awareness of the presence of an alarm
- Unacknowledged – when the alarm is raised but the operator has not indicated awareness of its presence
- Cleared – when the condition that triggered the alarm has returned to normal
- Shelved – the operator has prevented a nuisance alarm from being displayed for a limited time
- Suppressed – alarm is suppressed when logical criteria are applied to determine that the alarm shall not occur, even though the base alarm condition is present.

If an alarm clears before being acknowledged by the operator, the alarm remains in the alarm table – latched behaviour - but is presented in reverse-video (text font colour becomes background colour, and background colour is used for the alarm font).

4.2 Alarm Pane

The alarm pane reflects the alarm status of the controlled system displayed on the mimic. It is a standard component provided by CODAC. Figure 4-2 shows the integration of the alarm pane at runtime on the top right of the screen:

- Each alarm is presented in a single row
- To the left of each alarm there is an acknowledgement tick box
- Each alarm states (left to right):
  - Alarm priority symbol
  - Alarm description
  - Time
- The background colour of the alarm message reflects the priority of the alarm
- The colour of the alarm priority symbol reflects the priority of the alarm
- The alarm priority symbol flashes at 2Hz until acknowledged by the operator.
The alarm pane is limited to the 20 highest triggered alarms on the related CBS level (CBS filter).

4.3 Alarms List

The Alarms List standard component provides the operator with a list of all latched alarms and the functionality to navigate and view additional information about alarms.

A CODAC latched alarm is the first highest occurrence of an un-acknowledged alarm. If an alarm goes from minor to major state, the latched alarm will correspond to the major state, time and value. If an alarm flickers between cleared and alarm states, the latched alarm will correspond to the first time the alarm was triggered.

Each entry in an alarm list shows:

- Tick box to acknowledge the alarm,
- Alarm priority symbol,
- Alarm description,
- Date and time,
- Current severity and status. This information could be [OK – NO ALARM] if the condition that triggered the alarm has returned to normal. Such cleared alarm will remain in the list until acknowledged by the operator (latched behaviour) but will be displayed in reverse video,
- Alarm PV,
- Value of the setting transgressed,
- Alarm ID.

The background colour of the alarm message reflects the priority of the latched alarm and the alarm priority symbol flashes at 2Hz until acknowledged by the operator.

The alarms list as shown on Figure 4-3 is made available via a right-click on any navigation button and using the option Actions -> Open in a new window the Alarms List.
4.4 Alarm Coding

Alarm coding as illustrated on Figure 4-4 includes the background alarm sensitive alarm message, the alarm severity symbols or icons and the colour codes.

Cleared alarms remain in the alarm pane and alarms list until acknowledged by the operator (latched behaviour) but are displayed in reverse video i.e. the background colour of the severity is used for the foreground and vice-versa. For example, a MAJOR alarm message is displayed with a white font on a red background. If cleared, the message will appear with a red font on white background.

The icons represent the severity of the alarm – INVALID, MAJOR and MINOR. An active alarm acknowledged by the operator will be represented with a check box on the top right of the icon. A cleared alarm not yet acknowledged will have a (i) information indicator on the top right of the icon.

<table>
<thead>
<tr>
<th>Icons</th>
<th>Shelved alarms*</th>
<th>Colour</th>
<th>RGB colour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid/Unknown alarm</td>
<td></td>
<td></td>
<td>(255,0,255)</td>
</tr>
<tr>
<td>Major alarm</td>
<td></td>
<td></td>
<td>(250,15,14)</td>
</tr>
<tr>
<td>Minor alarm</td>
<td></td>
<td></td>
<td>(255,255,0)</td>
</tr>
</tbody>
</table>

* Shelved – the operator has prevented a nuisance alarm from being displayed for a limited time
Figure 4-4 Alarm Coding
4.5 Message History

The Message History as illustrated on Figure 4-5 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.

![Figure 4-5 Message History](image-url)