Notices and Trademarks

Copyright 2010 by Honeywell International Sárl.
Release 200.1  Apr 2017

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a particular purpose and makes no express warranties except as may be stated in its written agreement with and for its customers.

In no event is Honeywell liable to anyone for any indirect, special or consequential damages. The information and specifications in this document are subject to change without notice.

Honeywell and Experion PKS are registered trademarks of Honeywell International Inc.
Other brand or product names are trademarks of their respective owners.

Honeywell Process Solutions
1860 W. Rose Garden Lane
Phoenix, AZ  85027 USA
1-800 822-7673
Contact Information

Seeking technical assistance
For technical queries, contact Honeywell Customer Support.
For contact information, visit:

Reporting a security vulnerability
For the purpose of submission, a security vulnerability is defined as a software defect or weakness that can be exploited to reduce the operational or security capabilities of the software.
Honeywell investigates all reports of security vulnerabilities affecting Honeywell products and services.
To report a potential security vulnerability against any Honeywell product, follow the instructions at: https://honeywell.com/pages/vulnerabilityreporting.aspx.
Submit the requested information to Honeywell using one of the following methods:
• Send an email to security@honeywell.com.
• Contact your local Honeywell Technical Assistance Center (TAC).

Providing documentation feedback
To provide feedback about this document, or to report errors and omissions, write to us at:
hpsdocs@honeywell.com
# Contents

1. **INTRODUCTION** ........................................................................................................... 1
   1.1 About alarm management.......................................................................................... 1
       Life cycle of alarm management .............................................................................. 2
       Loops in the alarm management life cycle ............................................................... 5
   1.2 About the DynAMo alarm suite ............................................................................. 5
       Alarm Configuration Manager ................................................................................... 5
       Metrics & Reporting ................................................................................................. 6
       User Alerts .............................................................................................................. 6
   1.3 About Metrics & Reporting..................................................................................... 6

2. **GETTING STARTED** ................................................................................................. 9
   2.1 Layout of Metrics & Reporting screen ................................................................... 9
       Navigation pane ......................................................................................................... 9
   2.2 Reports .................................................................................................................. 11
       About Metrics & Reporting reports ...................................................................... 11
       Common controls ...................................................................................................... 11
       Filtering data in reports ........................................................................................... 12
       Exporting reports to PDF or Excel ......................................................................... 14
       Setting time range in reports .................................................................................. 15
       Adding comments to reports ................................................................................... 20
       Zooming the display of trends .................................................................................. 21

3. **ASSESSING ALARM PERFORMANCE** ................................................................. 23
   3.1 Assessing alarm performance .............................................................................. 23
   3.2 Assessing the overall health of your alarm system ............................................. 23
   3.3 Assessing operator-wise alarm performance ....................................................... 25
   3.4 Identifying the best & worst performing units ..................................................... 27
   3.5 Analyzing the alarm priority distribution .............................................................. 28
   3.6 Analyzing alarm performance overview .............................................................. 30

4. **REVIEWING DAY-TO-DAY OPERATIONS** .............................................................. 33
   4.1 Reviewing day-to-day operations ....................................................................... 33
7.4 Analyzing D&E alarm priorities ............................................................... 68
7.5 Identifying D&E unmanaged tags ......................................................... 70

8. VIEWING REAL-TIME MESSAGES .................................................... 71
8.1 Viewing real-time events ................................................................. 71
8.2 Viewing real-time alarms ................................................................. 73

9. REFERENCE TOPICS ............................................................................. 77
9.1 About symptomatic analysis .......................................................... 77
   Overview ............................................................................................... 77
   An illustration for symptomatic analysis .............................................. 77
9.2 Standing and stale alarms ............................................................... 79
9.3 Chattering and fleeting alarms ...................................................... 79
   Chattering Alarms .............................................................................. 79
   Fleeting alarms ................................................................................. 81
1. Introduction

1.1 About alarm management

**What is an alarm?**
An alarm is an audible and/or visible means of indicating to the operator an equipment malfunction, process deviation, or abnormal condition requiring a response. (ISA-18.2)

Automation systems installed in process plants generate thousands of alarms every day. These alarms can be categorized into two types - nuisance alarms and critical alarms. Nuisance alarms are alarms that arise from day-to-day activities such as the opening of an electrical switch room door. Nuisance alarms do not require any operator action. Critical alarms are alarms that indicate a critical equipment failure, an operating problem, and/or a potential safety risk.

Control room operators review the alarms individually, identify the critical ones, and respond to them appropriately. As a result, the operators are always busy reviewing thousands of alarms every day. A proper alarm management system helps reduce this workload (of the operators) by automatically identifying and filtering out nuisance alarms.

According to the Abnormal Situation Management (ASM) Consortium, ineffective management of nuisance alarms can lead to incidents that cost the process industry billions of dollars, and pose an increased risk of fatigue and stress for operators who must constantly make instant decisions on how to respond to an alarm. When operators are forced to deal with hundreds of alarms at any given point in time, there is increased risk to safety and process efficiency.

**What is alarm management?**
Alarm management is the process by which alarms are engineered, monitored, and managed to ensure safe and reliable operations.
Life cycle of alarm management

For any factory or site, alarm management is a continuous cyclic process. The life cycle of alarm management consists of ten stages as shown below (Adapted from the ISA-18.2 Alarm Management Life Cycle):

- Some stages may be executed simultaneously rather than sequentially. For example, Management of Change is performed for stages Identification, Rationalization, Detailed design, and Implementation.
- In some cases, one of the stages may be skipped. For example, during a rationalization exercise the outcome may be a simple change in alarm setting, which may not require a detailed design to implement.
**Philosophy**

This is the first step towards deploying an alarm management system at your plant/site. In this phase, you create an alarm philosophy document that provides high level guidelines about your plant/site's approach to managing alarms.

The alarm philosophy document typically contains:

- The rules for categorizing the alarms (based on their characteristics, and the requirements for training, testing, documentation, or data retention)
- The rules for prioritizing the alarms (based on consequence rating & response time)
- The color coding for displaying the alarms in the human-man interface (HMI) screens
- The workflow for the Management of Changes (MOC) in the alarm definitions
- The key performance benchmarks for the alarm system (Eg. number of alarms that an operator can handle in an hour)
- Roles and responsibilities of the people involved

The alarm philosophy document is a mandatory requirement for alarm management as per industry standards.

The DynAMo Alarm Suite (Alarm Configuration Manager and Metrics & Reporting) helps you with this phase of the alarm management life cycle.

**Identification**

In this phase, you identify the potential alarms. Following are a few exercises that can help you identify the potential alarms:

- Process Hazard Analysis (PHA)
- Incident investigations
- Hazard and Operability Study (HAZOPS) / Control Systems Hazard and Operability Study (CHAZOPS)
- Alarm design/rationalization workshops

The DynAMo Alarm Suite (Alarm Configuration Manager) help you with this phase of the alarm management life cycle.

**Rationalization**

Now that you have identified the potential alarms, you can review whether each alarm confirms to the rules defined your alarm philosophy document.

You can then validate whether each identified alarm qualifies as an alarm by asking yourself the following questions:

- Does it indicate an abnormal condition?
- Does it require an operator action?
- Is it unique (or a duplicate of another alarm)?

After qualifying the alarms, you must capture the following details for each alarm:

- Description of the alarm
- Configuration settings
- Causes for the alarm
- Consequences of no action
- Required operator action
- Response time
About alarm management

- Consequence rating (the severity of its consequences)
- Priority of the alarms

Rationalization helps you in identifying the minimum number of alarms that enable the plant/site to operate safely. This ensures that a control room operator gets to see only the critical alarms that he needs to act upon, rather than having to go through a huge list of alarms and trying to identify the one that needs his attention.

The DynAMo Alarm Suite (Alarm Configuration Manager) help you with this phase of the alarm management life cycle.

Design
During this phase, you setup your alarm management system based on the information that you created during the rationalization. This stage involves:
- Configuring the alarms in the control system
- Setting up the Human Machine Interface (HMI) for the control room operator to view the alarms

The DynAMo Alarm Suite (Alarm Configuration Manager) help you with this phase of the alarm management life cycle.

Implementation
In this stage, you put your alarms into service. This stage involves:
- Testing of the alarm system functions
- Relevant training for the operators and other personnel

The DynAMo Alarm Suite (Alarm Configuration Manager) help you with this phase of the alarm management life cycle.

Operation
The alarm is now in service and is reporting abnormal conditions to the operator.
The DynAMo Alarm Suite (Metrics & Reporting) help you with this phase of the alarm management life cycle.

Maintenance
Process measurement instruments, final control elements, and control systems all require periodic/predictive maintenance to ensure their continued reliable operation. This is critical to ensure the ongoing performance of the alarm system.
The DynAMo Alarm Suite (Metrics & Reporting) help you with this phase of the alarm management life cycle.

Monitoring & Assessment
This stage includes the periodic collection and analysis of data from alarms. Without monitoring it is virtually impossible to maintain an effective alarm system. Assessment should be undertaken frequently (daily or weekly) and is the primary method for determining problems such as nuisance alarms, stale alarms, and alarm floods.
The DynAMo Alarm Suite (Metrics & Reporting) help you with this phase of the alarm management life cycle.

Management of Change (MOC)
Management of change is a critical stage that helps ensure the ongoing integrity of the alarm system. It needs to be a structured process of approval and authorization for any additions, modifications, and deletions of alarms from the system.
The DynAMo Alarm Suite (Alarm Configuration Manager) help you with this phase of the alarm management life cycle.

**Audit**

A periodic audit of the alarm system and the processes detailed in the alarm philosophy may determine the need to modify processes, the philosophy, or the design etc. This is also the ideal stage to enter the alarm system life cycle process. The audit may also highlight that an organization’s discipline to follow the processes (especially MOC) may need improvement.

**Loops in the alarm management life cycle**

There are three “loops” in the alarm management life cycle as represented by the dotted lines in above figure.

- **Monitoring & Maintenance loop** - This loop is typically applied for simple maintenance-related issues. If an alarm issue is detected in the "Monitoring & Assessment" stage then it would be resolved via this loop (for example, resolving the chattering alarms).
- **Monitoring & Management of Change (MOC) loop** - This loop is used to resolve complex issues that require design level changes in your alarm system.
- **Auditing & Philosophy loop** - This loop basically entails the whole life cycle process. Periodic audits of your alarm system is a mandatory requirement as per industry standards.

### 1.2 About the DynAMo alarm suite

The DynAMo Alarm Suite is an effective tool for optimizing your alarm management strategy to prevent alarm floods and 'chatter', and reduce operator stress. The suite offers a layer of protection to minimize unplanned outages, safety incidents, and environmental releases. DynAMo Alarm Suite increases operator effectiveness by reducing the alarm count and helping operators focus and respond to the most critical alarms. The software suite leverages more than 20 years of alarm management experience in the process industries to help users reduce overall alarm count by as much as 80%, identify maintenance issues, and increase visibility of critical alarms that require urgent attention.

Other features of the suite include:

- Compliance with global safety standards
- Compliance with Abnormal Situation Management (ASM) Consortium best practices
- Customizable mobile device-compatible dashboard to view the health of the alarm system at a glance
- Integration with all major distributed control systems (DCS) in the industry

DynAMo Alarm Suite brings together key software for a comprehensive solution to increase safety and operator efficiency. A combination of tools for alarm monitoring, enforcement, and alerting and notification offers you a single, simple solution that includes our most powerful advanced applications for effective alarm management.

The suite consists of 3 software components:

- Alarm Configuration Manager
- Metrics & Reporting
- User Alerts

**Alarm Configuration Manager**

Alarm Configuration Manager helps you to engineer an alarm system to meet the alarm management policies of your site and to safeguard your plant and its processes. It is a vendor-neutral software that allows you to create and maintain a master alarm and boundary database for your distributed control system (DCS). This database acts as a centralized repository for all alarm configuration and documentation, and ensures that the configuration remains in effect over the life cycle of the plant.

It allows you to import alarm configuration information from DCS, human machine interfaces (HMIs), PLCs and other systems. It also allows mode-based alarming via its documentation and rationalization
functions, and assists in optimizing the alarm system to increase operator efficiency. ACM is compatible with all major control systems available in the industry.

Key benefits of ACM include:

- Reduced time and effort to develop, deploy and maintain an alarm system consistent with best practices defined by the Abnormal Situation Management (ASM) Consortium
- Reduced risk of process upsets due to invalid alarm system parameters
- Improved regulatory compliance
- Sustained alarm system performance

**Metrics & Reporting**

Metrics & Reporting is a software application that collects alarm and event data from various data sources, and presents the data in the form of intuitive reports to help you gain valuable insight into your plant's performance. The application also helps you to visually compare your alarm metrics against industry standards, and identify the deviations within seconds.

By analyzing your alarms and comparing them against the standards, you can:

- Identify and respond to abnormal situations quickly and easily
- Gain insights into your plant’s performance based on historical facts
- Filter out irrelevant alarms, allowing operators to focus on the alarms that pose a significant safety or financial risk
- Achieve an alarm management model that improves operational performance while meeting regulatory compliance and safety standards
- Improve the productivity of your plant

**User Alerts**

User Alerts is a software application that notifies when pre-defined, time-based, and process value-based conditions are met. Designed to complement the process control alarm system, it is intended to handle process conditions where notifying operators is useful but alarms are not appropriate. It provides a way to detect and annunciate process value exceedances and conditions that are of a lower level of importance than true alarms.

UA is primarily a plant control function, intended for operators, and other support personnel involved in control room operations. The automatic notification helps prevent abnormal events and ensure that required tasks are not forgotten. It provides near-real time alerting and notification for conditions when process data is outside of process limits and reduces risks by escalating unconfirmed events to the appropriate people.

Benefits of UA include:

- Improved operator effectiveness
- Reduced alarm flooding
- Enables early detection of abnormal situations
- Increased unit integrity and operator confidence

**1.3 About Metrics & Reporting**

Metrics & Reporting is a software application that collects alarm and event data from various data sources, and presents the data in the form of intuitive reports to help you gain valuable insight into your plant's performance. The application also helps you to visually compare your alarm metrics against industry standards, and identify the deviations in seconds.
**Benefits of Metrics & Reporting**

Metrics & Reporting helps you with the following 4 phases of the alarm management life cycle:

- **Philosophy:**
  In this phase, you can use Metrics & Reporting to:
  - Configure metric definitions - Copy metric definitions from industry standards and modify them as required
  - Configure metric settings - Use the default threshold values for the metrics, or modify the threshold values

- **Operation:**
  In this phase, Metrics & Reporting helps you to:
  - **Review day-to-day operations** - Perform thorough and easy incident investigation using the reports. This is one of the key safety requirements as per industry standards and regulatory bodies.

- **Maintenance:**
  In this phase, you can use Metrics & Reporting to:
  - **Resolve bad actors** - Identify improvement opportunities in your alarm configuration, instrumentation problems in your control system, and automation opportunities in your plant.
  - **Analyze and investigate events** - A significant chunk of alarms might arise due to unforeseen loop-holes in your process. You can identify these alarms and their root causes, and bring in process changes to prevent re-occurrence of such alarms. In other words, you can continuously make incremental improvements to your process, and make your process better and better every day.

- **Monitoring & Assessment:**
  In this phase, you can use Metrics & Reporting to:
  - **Assess alarm performance** - Analyze how your operators are loaded and whether appropriate alarms are raised for all the scenarios. A quick glance at the reports tells you where your key alarm performance indicators (KPIs) stand against industry standards.

**Components of Metrics & Reporting**

Metrics & Reporting is a collection of software components that work together as one application.

The components of Metrics & Reporting are:

<table>
<thead>
<tr>
<th>Component of M&amp;R</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core App</td>
<td>Hosts the business logic of the Metrics &amp; Reporting application</td>
</tr>
<tr>
<td>Core Web</td>
<td>Hosts the Metrics &amp; Reporting application (as a website)</td>
</tr>
<tr>
<td>Archiver</td>
<td>The Archiver:</td>
</tr>
<tr>
<td></td>
<td>- receives event data from the Collector</td>
</tr>
<tr>
<td></td>
<td>- manipulates the data into meaningful information with the help of the post-processing script and rules file</td>
</tr>
<tr>
<td></td>
<td>- archives the data into a database</td>
</tr>
<tr>
<td></td>
<td>When you install the Archiver, a new event data archive database is created.</td>
</tr>
<tr>
<td>Database</td>
<td>Installs the following databases to store the configuration data:</td>
</tr>
<tr>
<td></td>
<td>- platform (Honeywell.CoreSystem)</td>
</tr>
<tr>
<td></td>
<td>- shift rotations (Honeywell.Shifts)</td>
</tr>
<tr>
<td></td>
<td>- asset model (Honeywell.MES.AssetTask.DataModel.AssetTaskDataModel)</td>
</tr>
<tr>
<td></td>
<td>Other Metrics &amp; Reporting configuration (Honeywell.DynAMo.Alarms)</td>
</tr>
<tr>
<td>Collector</td>
<td>The Collector:</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------</td>
</tr>
<tr>
<td></td>
<td>• collects alarm and event data from event data sources (DCS/PLC/ESD/BMS etc.) through various modes (OPC AE / ODBC / Serial / File)</td>
</tr>
<tr>
<td></td>
<td>transfers the collected data to the Archiver</td>
</tr>
</tbody>
</table>

You can install all the components of M&R on a single computer or across computers and configure them to connect with each other and work synchronously.
2. Getting started

2.1 Layout of Metrics & Reporting screen

The major sections of the Metrics & Reporting screen are:

- **Navigation pane** - displays the options to navigate to any Metrics & Reporting screen
- **Content area** - displays the actual content of the screen. For example, in the Chattering Alarms screen, the content area of the screen displays the Chattering Alarms report.
- **Action bar** - displays the page title and contains options to display the navigation & filtering panes, set the time range for analysis, export current page to Excel or PDF, add comments, and perform additional screen-specific tasks

**Navigation pane**

The Navigation pane displays the options for navigating to any Metrics & Reporting screen.
The pane contains the following icons:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✷</td>
<td>Displays options to launch your favorite reports. <strong>ATTENTION:</strong> You can add any report to the Favorites list by clicking the Add to Favorites option as shown below:</td>
</tr>
<tr>
<td></td>
<td>Opens the Metrics &amp; Reporting dashboard</td>
</tr>
<tr>
<td></td>
<td>Displays options to launch your User Reports (based on your login user account)</td>
</tr>
<tr>
<td></td>
<td>Displays options to launch the standard reports</td>
</tr>
<tr>
<td></td>
<td>Displays the options to launch the advanced reports</td>
</tr>
<tr>
<td></td>
<td>Displays options to launch the custom reports that you created/imported</td>
</tr>
<tr>
<td></td>
<td>Displays options to launch the administrative screens</td>
</tr>
<tr>
<td></td>
<td>Opens the <strong>Configuration</strong> screen</td>
</tr>
<tr>
<td></td>
<td>Opens the DynAMo Metrics &amp; Reporting Help Center</td>
</tr>
</tbody>
</table>

**Action bar**

Displays the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Name of the option</th>
<th>Description</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 days before now</td>
<td>Set time range</td>
<td>Allows you to specify a time range for the messages to be analyzed.</td>
<td><a href="#">Setting time range in reports</a></td>
</tr>
<tr>
<td>Export</td>
<td>Exports page contents to a PDF file or Excel sheet.</td>
<td><a href="#">Exporting reports to PDF or Excel</a></td>
<td></td>
</tr>
<tr>
<td>Comment</td>
<td>Allows you to add comments to the current page.</td>
<td><a href="#">Adding comments to reports</a></td>
<td></td>
</tr>
<tr>
<td>Filter</td>
<td>Displays the filtering pane</td>
<td><a href="#">Filtering data in reports</a></td>
<td></td>
</tr>
<tr>
<td>Sequence of events</td>
<td>Displays the sequence of events</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2.2 Reports

About Metrics & Reporting reports

In some scenarios, we find it necessary to switch between two or more reports several times to identify a problem and its root cause. Whenever you find yourself in such a scenario with your alarm problems, the reports in Metrics & Reporting will be of great help. These reports are designed to help you in quickly identifying problems and their root causes without having to switch between views.

Each report contains a logical grouping of metrics (displayed as graphical plots, barcharts, or tables) focused to solve a specific problem. A report contains one primary metric or information, which is supported by two or more secondary metrics related to it. For example, the Bad Actor report displays 5 metrics - Most frequent alarms, Most frequent actions, Chattering alarms, Fleeting alarms, and Symptomatic analysis.

The block that represents each metric (plot/barchart/table) in the report is referred to as a widget. The widgets in a report are smart and interconnected. The interactive changes that you perform in one widget are automatically reflected in other widgets in the reports. When you select an item (row/bar) in one of the widgets (table/barchart/graph), all the remaining widgets in the report are automatically refreshed to show the selected item (if it exists) in the highlighted mode. In a single click, you can quickly identify whether or not a particular item is featured in two or more metrics. This automatic highlighting helps you easily visualize, analyze, and understand the impact of a specific item on different metrics.

Common controls

While analyzing a problem, if you want to view additional information about a specific item, you can select to view additional contextual information like Sequence of Events, Alarm Properties etc along with filters like time, asset, events, tags etc.

Above every widget (graph/barchart/table) in the reports, you can find some or all of the following icons:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✪</td>
<td>Switch from barchart view to tabular view.</td>
</tr>
<tr>
<td>✫</td>
<td>Switch from tabular view to barchart view.</td>
</tr>
</tbody>
</table>
Icon | Description
--- | ---
| Display alarm documentation for the selected tag
| When an alarm occurs, you need more information about the alarm such as the potential causes of the alarm, the potential impact, the containment and corrective actions you must take to bring the situation back to normalcy, etc. This information is called alarm documentation. Typically, alarm documentation is captured at the time of alarm configuration.
| Display the Sequence of Events for the selected tag
| Sequence of Events is a listing of all the alarms & events related to a specific tag, listed in the sequence of their occurrences.

**Filtering data in reports**

The reports in DynAMo Metrics & Reporting allow condition-based filtering of messages. In other words, you can specify conditions to filter out unwanted messages and display only the messages that you want to view in the reports.

**Default filters**

When you open any report in Metrics & Reporting, the following filters are applied by default:

- Suppressed - no
- Shelved - no
- Priority - not equal to journal

To modify the default filters or specify additional filtering criteria:

1. On any Metrics & Reporting report, click ☰.

   ![filter_icon]

   The **Filters** pane appears.

2. The options in the **Asset** group allow you to filter and display only the messages that originate from specific sites, plants, or operator positions. The tree view displays the asset hierarchy of your site. Specify your filtering criteria by selecting or clearing the check boxes in the tree nodes.
   - To filter the data based on assets, click ☰ icon and select the assets.
• To filter the data based on operator positions, click the icon and select the operator positions.

3. To filter the data by Tag Name, Identifier, Priority, Block Name, Suppressed status, Shelved status, Tag Description, System Input Name, Visibility, or Filter columns, you must expand the appropriate section in the Filters pane.

The two fields in this section allow you to specify your condition as a phrase:

• The drop-down list allows you to select the comparison operator. The available options are:
  • Contains
  • Starts with
  • Ends with
  • Equals
  • Does not contain
  • Does not equal
• The text field allows you to type the filter text.

For example, if you want to filter by tag names that start with "HIGH", then expand the Tag Name section, select Start with in the drop-down list, and specify HIGH in the text field.

ATTENTION:
The filtering is not case-sensitive.

4. Click the + button to add the filtering criteria.
5. Similarly, you can add one or more filtering criteria.

The behavior of the filters differ based on the conditions you create:

If different conditions involve different parameters, the "AND" operator is used.
Example: If you add two filtering conditions - "Tag Name starts with AB02" and "Priority equals 4", then the report displays the events for which both these conditions are true.

If two or more conditions involve the same parameter, the "OR" operator is used.
Example: If you add two filtering conditions - "Tag name starts with AB02" and Tag name contains RTR", then the report displays events for which the Tag name starts with AB02, and also the events for which tag name contains RTR.

6. Click

The widgets in the report refresh themselves and display the filtered data.
ATTENTION:
Depending on the data shown in the reports, the filtering options may vary. In some reports, some of the filtering options defined in this section may not be available.

TIP:
- If filter is applied, the filter icon appears in blue color ( ). It also displays a number that indicates how many filters are currently applied.
- The currently applied filters are highlighted in blue color:

![Filter Icons](image)

Exporting reports to PDF or Excel
You can export the contents of any Metrics & Reporting report to a PDF file or a Microsoft Excel spreadsheet.

To export the current view:

1. On any Metrics & Reporting report, click and then click Export to Excel or Export to PDF. The Export dialog box appears.

![Export Dialog Box](image)

2. Specify the destination folder and the file name for the exported Excel or PDF file.
3. Click Export.
A PDF or Excel file is created at the specified location with the contents of the current Metrics & Reporting page.
If you are using Windows Server operating systems, you can export reports to PDF or Excel only if you have disabled Enhanced Security.

**Setting time range in reports**

By default, the reports display metrics & KPIs corresponding to a specific time range. This default time range is automatically calculated depending on the available data. However, you can modify this time range and view the metrics & KPIs corresponding to any custom time range.

**ATTENTION:**
The data shown in the Metrics & Reporting screens are based on the site's time zone (that is configured in the Archiver).

The time control allows you to specify:
- a time range - can be used to analyze data for that time range
- a specific moment (a single point in time) - can be used to analyze data for a specific moment (e.g., standing and stale alarms at 29-Nov-2015 10:00:00 AM). This option is not available for all the reports
- slice the report data - can be used to chunk of the data to be analyzed. This options is not available for all the reports.

The time control on report screens allow you to set the time range for the metrics & KPIs displayed in that report.

![Time control example](image)

**Selecting a time range**

**Selecting an adjacent time range**
The time control displays the selected time range.

To use an adjacent time range of the same duration click the previous or next icons.

![Adjacent time range example](image)

For example, if the time control displays “7 days from now”:
- Click previous to select the 7 days prior the the last 7 days
- Click next to select the 7 days after now

**Specifying start time and end time**
To select the time range by specifying the start and end date & time:
1. Click the time range displayed in the time control.
2. Expand the **Date & Time** group.

3. Type the start and end dates & times in the appropriate boxes. You can also select the date and time by clicking calendar and time icons respectively.

**Selecting a relative time range**

To select a relative time range (in the format **25 days before 3-Jun-2015 09:30:00**):

1. Click the time range displayed in the time control.
2. Expand the **Relative Time** group.

3. In the date box, specify the base date and time.

   - **OR**
   - To specify the current date and time, select the **Now** check box.

4. In the drop-down list, click the appropriate relation.
   The available options are **before**, **centered on**, and **after**.
5. Using the duration fields, specify the duration of the time range.

![Duration Fields Example]

**Selecting a default time range**

Metrics & Reporting provides some default relative time ranges that you can readily access and use.

- 8 hours before now
- 12 hours before now
- 24 hours before now
- All of today
- All of yesterday
- 7 days before now
- Start of the week to now
- All of last month
- 3 months before now

To select a default time range:

1. Click the time range displayed in the time control.
2. Expand the **Shortcuts** group.

3. Select the required shortcut.

**Selecting a specific moment**

To select a specific point in time, click the **Single tab** and specify the time as explained in the above sections.

**ATTENTION:**

Selecting a specific moment is only applicable for the **Standing and Stale** report.
Slicing the report data

In the barcharts and graphical trends where data is plotted against time, you can define the chunking size of the data using the slicing drop-down list of the time control.

For example, consider a report where a barchart displays the alarm count for the last month. Each bar in the barchart represents the alarm count for a day. If you want to see a barchart showing the alarm count grouped by weeks, click Week in the slicing drop-down list of the time control.

ATTENTION:
While analyzing data for two or more plants with different shift rotations, you cannot slice the data by shifts.

The slicing options vary depending upon the time range that you select.
For example:
- If you select a time range more than a month, the slicing options available are Month and Week.
- The option to slice by shifts is available only if the selected time range is less than a week.

Adding comments to reports

You can also view a log of all the comments added to this report by all your users.

ATTENTION:
- Comments added cannot be modified or deleted.
- While accessing Metrics & Reporting from another domain (L4/Business Network), you can only view the comments. You cannot add new comments.

1. On the Metrics & Reporting dashboard or any report screen, click the icon.

![Comment icon]

The Comments pane appears.

2. To add a comment, click the Add Comment icon.

![Add Comment icon]
3. In the New Comment box, type your comment and click .
   The new comment is added to the report and displayed in the Comments pane.
   The Comments pane list displays the comments added by other users as well.

4. To reply to a comment, click the Reply icon, type the comment and click .

   ![Comments pane](image)

**Zooming the display of trends**

In the reports that contain graphical trends plotted against time, you can zoom the graph for a more closer look.

To zoom a graph:

1. Drag your mouse over the graph to select the region that you want to zoom.

   ![Zooming graph](image)
2. When you finish dragging (release the mouse pointer), the graph zooms in.

3. To zoom out to the original size again, click **Reset Zoom**.
3. Assesing alarm performance

3.1 Assessing alarm performance

Alarm management is a continuous process. You must regularly monitor the performance of your alarm system. This will help you identify improvement opportunities in your process and alarm configurations.

In a healthy alarm system, operators are optimally loaded and appropriate alarms are raised for all the scenarios. This can be achieved by calculating the key alarm performance indicators (KPIs) and comparing them against the industry standards. Metrics & Reporting provides reports that help you display quantitative and qualitative tracking information.

DynAMo Metrics & Reporting helps you assess the performance of alarm system in different ways:

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Tools used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessing overall alarm performance</td>
<td>Metrics &amp; Reporting dashboard</td>
</tr>
<tr>
<td>Assessing operator-wise alarm performance</td>
<td>Alarm Performance Indicators report</td>
</tr>
<tr>
<td>Identifying best &amp; worst performing units</td>
<td>Tree Map Risk Assessment report</td>
</tr>
<tr>
<td>Assessing alarm priority distribution</td>
<td>Alarm Priority Distribution report</td>
</tr>
<tr>
<td>Analyzing alarm performance overview</td>
<td>Alarm Performance Overview report</td>
</tr>
</tbody>
</table>

3.2 Assessing the overall health of your alarm system

You can get a quick overview of the overall health of the alarm system using the Metrics & Reporting dashboard. It helps you to quickly and easily identify the metrics that deviate from the target.

To assess the overall health of your alarm system:

1. From any Metrics & Reporting screen, click on the left of the screen.

   The dashboard appears.

2. To understand how your alarm system is performing, see the Alarm performance for the current day section of the dashboard.

<table>
<thead>
<tr>
<th>Alarm Performance</th>
<th>Today</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Overloaded</td>
<td>Predictive</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Reactive</td>
<td>Robust</td>
</tr>
<tr>
<td>2</td>
<td>Stable</td>
</tr>
</tbody>
</table>

   The numbers in this section specify how many of your operators are currently experiencing Overloaded, Reactive, Stable, Robust, and Predictive alarm performance.

3. To know how many alarms are currently open, and their priority-wise break-up, see the Open alarms for the current day section.
4. To analyze your key alarm performance indicators (KPI) in detail, refer to the KPI Trends section.

To view only the deviated KPIs, select Show Deviation only.

The list of KPIs displayed depends on your user privileges configured by your system administrator. See the topic Configuring user accounts for details on configuring user privileges.

**ATTENTION:**
The following KPIs display the average values for all operators for the "current moment" (not across a time range):

- Average Standing Alarms
- Average Stale Alarms

**ATTENTION:**
Sometimes, the dashboard may report some KPIs as deviated (highlighted in red color) though the KPI value is within the normal range. This is because, the KPI value displayed in the dashboard is the average value across all operator positions. Though the average value is within the range, if the KPI value for one of the operator positions is not in the normal range, it appears highlighted in red color.

5. By default, the KPI trends for the last 7 days are displayed. To display the trends for the last 13 weeks, click Weekly.

Use the and icons to navigate back and forth in time. You can also use the slider (in between these two icons) to navigate back and forth in time.

6. To view more details about a specific KPI, click the name of the corresponding widget in the dashboard. For example, if you want to know more details about the Average Standing Alarms, click the heading (Average Standing Alarms) to open the Alarm Performance Overview report and view more details about the average standing alarms for the same time range that you selected in the dashboard.
7. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the data that you want to view and analyze</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>Note: Unlike the other reports, the Metrics &amp; Reporting dashboard allows you to filter the data based on only one parameter - Priority.</td>
<td></td>
</tr>
<tr>
<td>Add comments to the current view</td>
<td>Adding comments to reports</td>
</tr>
</tbody>
</table>

3.3 **Assessing operator-wise alarm performance**

Take a quick glance at the Alarm Performance Indicators report and you will know how well your alarm system is performing for each of your operator positions. The report tells you how many of your operator positions are experiencing the alarm performance as Overloaded, Reactive, Stable, Robust, and Predictive. It helps you find answers to the following queries:

- How well is my alarm system performing for each operator position?
- How is the performance for each operator position versus the average?

To assess alarm performance indicators:

1. From any Metrics & Reporting screen, click on the left of the page.
   The Standard Reports pane appears.
2. Click **Alarm Performance Indicators**.
   The **Alarm Performance Indicators** report appears.
   **TIP:** Alternatively, you can open this report by clicking the Alarm performance for the current day section in the dashboard.

   The primary metric displayed in this report is Alarm Performance Indicator, and the secondary metrics are peak alarm rate, percentage upset, and average alarm rate. The Alarm Performance Indicator is calculated

3. The numbers on the top-right corner of the screen (highlighted in the image below) specify how many of your operators are currently experiencing Overloaded, Reactive, Stable, Robust, and Predictive alarm performance.

   ![Alarm Performance Indicators](image)

   This is a measure of how your operators are loaded by your alarm system in the real-time, graded against industry guidelines. Best practices recommend operating in a Stable state, with occasional results of Robust.
4. In the **Alarm Performance Indicators** table, each row represents an operator position.

The **Performance** column displays the performance category of each operator position.

This performance category is calculated from three metrics as shown below:

<table>
<thead>
<tr>
<th>Performance category</th>
<th>Average alarm rate per 10 min</th>
<th>Peak alarm rate per 10 min</th>
<th>% Time &gt; 5 Alarms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overloaded</td>
<td>&gt;100</td>
<td>&gt;1000</td>
<td>&gt;50%</td>
</tr>
<tr>
<td>Reactive</td>
<td>10 - 100</td>
<td>&gt;1000</td>
<td>25 - 50%</td>
</tr>
<tr>
<td>Stable</td>
<td>1 - 10</td>
<td>100 - 1000</td>
<td>5 - 25%</td>
</tr>
<tr>
<td>Robust</td>
<td>1 - 10</td>
<td>10 - 100</td>
<td>1 - 5%</td>
</tr>
<tr>
<td>Predictive</td>
<td>&lt;1</td>
<td>&lt;10</td>
<td>&lt;1%</td>
</tr>
</tbody>
</table>

5. The second half of the report shows graphical plots of the 3 API metrics, plotted against time. The orange lines in the plots represent the aggregate values.

6. To analyze about a specific operator position, click the corresponding row in the **Alarm Performance Indicators** table.

In addition to the existing orange lines, the graphs display blue lines that represent the metrics for the selected operator position.

This allows you to easily compare the metrics of an operator position against the aggregated metrics.

**ATTENTION:**

You can select only one operator position at a time.

7. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the data that you want to view and analyze</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>Set the time range for the data to be analyzed</td>
<td>Setting time range in reports</td>
</tr>
</tbody>
</table>
### 3.4 Identifying the best & worst performing units

If you want to identify which of your plants/areas had the best and worst alarm performance during a specific time range, the **Tree Map Risk Assessment** report can help you.

**ATTENTION:**

The **Tree Map Risk Assessment** report identifies relative, not absolute performance. It is best to have an understanding on whether a problem exists or not before using this report.

To analyze the units with the best & worst alarm performance:

1. From any Metrics & Reporting screen, click on the left of the page. The **Advanced Reports** pane appears.
2. Click **Tree Map Risk Assessment**.
3. By default, the size of the blocks in the block diagram are based on the total alarm count. To redraw the block diagram by using a different metric to define the size of the blocks, click that metric in the **Size** drop-down list.

In the above example, the site **SampleSite2** has two plants under it - **Plant1** and **Plant0**. The block diagram shows two regions representing the two plants. In the block diagram, the percentage area under each region represents the alarm count in that area based on the specified filtering criteria.

3. By default, the size of the blocks in the block diagram are based on the total alarm count. To use a different metric for representing the colors, click that metric in the **Color** drop-down list.

4. The scale below the block diagram shows the values represented by each color in the block diagram. By default, the values displayed in the scale are for the total alarm count. To use a different metric for representing the colors, click that metric in the **Color** drop-down list.
5. To modify the filtering criteria for the data shown in the report, drag the sliders on the left of the report.

6. To view the KPIs corresponding to one of the blocks in the block diagram, move your mouse-pointer over that block.

7. To drill-down and view the block down at the operator position level, click the name of the plant within the block.
   
   To return back to the site level, click the name of the site in the bread-crum link as shown below:

8. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the data that you want to view and analyze</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>Set the time range for the data to be analyzed</td>
<td>Setting time range in reports</td>
</tr>
<tr>
<td>Add comments to the current view</td>
<td>Adding comments to reports</td>
</tr>
</tbody>
</table>

### 3.5 Analyzing the alarm priority distribution

If you need to analyze how your alarms are distributed priority-wise, use the **Alarm Priority Distribution** report.

To analyze the alarm priority distribution:

1. From any Metrics & Reporting screen, click **Standard Reports** on the left of the page.
   
   The **Standard Reports** pane appears.

2. Click **Alarm Priority Distribution**.
The **Alarm Priority Distribution** report appears and displays a pie chart that shows how your alarms are distributed priority-wise.

### Priority Distribution

<table>
<thead>
<tr>
<th>Priority</th>
<th>Percentage</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Urgent</td>
<td>42.12</td>
<td>102,419</td>
</tr>
<tr>
<td>Low</td>
<td>30.16</td>
<td>116,309</td>
</tr>
<tr>
<td>High</td>
<td>27.72</td>
<td>106,872</td>
</tr>
</tbody>
</table>

3. Click a priority type in the legend area to view the pie chart again without that priority type.

For example, if you do not want to view High priority alarms in the pie chart, click HIGH in the legend area. To include the HIGH priority alarms in the pie chart again, click HIGH in the legend area again.

4. The table displays the percentage distribution for each priority and the number of alarms under each priority type.

5. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the data that you want to</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>view and analyze</td>
<td></td>
</tr>
<tr>
<td>Set the time range for the data</td>
<td>Setting time range in reports</td>
</tr>
<tr>
<td>to be analyzed</td>
<td></td>
</tr>
<tr>
<td>Add comments to the current view</td>
<td>Adding comments to reports</td>
</tr>
<tr>
<td>Export the report to Excel or PDF</td>
<td>Exporting reports to PDF or Excel</td>
</tr>
</tbody>
</table>
3.6 Analyzing alarm performance overview

You can analyze your Key alarm Performance Indicators (KPIs) operator position-wise using the Alarm Performance Overview report.

To analyze alarm performance overview:

1. From any Metrics & Reporting screen, click on the left of the page. The Standard Reports pane appears.
2. Click Alarm Performance Overview. The Alarm Performance Overview report appears and displays the KPIs for each operator position. The KPI values are sliced based on the slicing duration you have specified.
   - The KPI [Threshold] column displays the name of the KPI along with its threshold value (where applicable).
   - The deviations (values that exceed the threshold value) are highlighted in red.

ATTENTION:
- The report can display the metrics for up to SIX operator positions only. If you select 7 or more operator positions in the filtering pane, the report randomly displays any 6 of the selected operator positions.
- The following KPIs display the average values for all operators for the "current moment" (not across a time range):
  - Average Standing Alarms
  - Average Stale Alarms
3. In the **Select KPI** drop-down list, select the KPIs that you want to view in the report.

![Select KPI dropdown list](image)

4. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the data that you want to view and analyze</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>Set the time range for the data to be analyzed</td>
<td>Setting time range in reports</td>
</tr>
<tr>
<td>Add comments to the current view</td>
<td>Adding comments to reports</td>
</tr>
<tr>
<td>Export the report to Excel or PDF</td>
<td>Exporting reports to PDF or Excel</td>
</tr>
</tbody>
</table>
4. Reviewing day-to-day operations

4.1 Reviewing day-to-day operations

DynAMo Metrics & Reporting helps you review your day-to-day operations in different ways as follows:

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Tools used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyzing operator actions</td>
<td>Operator Response report</td>
</tr>
<tr>
<td>Analyzing chattering alarms list</td>
<td>Chattering Alarms List report</td>
</tr>
<tr>
<td>Assessing standing &amp; stale alarms</td>
<td>Standing &amp; Stale report</td>
</tr>
<tr>
<td>Analyzing shelved &amp; suppressed alarms</td>
<td>Shelved &amp; Suppressed report</td>
</tr>
<tr>
<td>Analyzing operator activity</td>
<td>Operator Activity report</td>
</tr>
</tbody>
</table>

4.2 Analyzing operator responses

If your operators spend most of their time responding to the same few alarms again and again, then something is wrong. If you get to know which few alarms keep your operators occupied all the time, you can investigate more and find out what is wrong. This analysis helps in identifying control system problems and automation options in your plant. After identifying the root causes the problems, you can resolve them.

The Operator Response report helps you analyze the pattern in which your operators respond to alarms.

To analyze operator responses:

1. From any Metrics & Reporting screen, click on the left of the page. The Advanced Reports pane appears.
2. Click Operator Response. The Operator Response report appears.
3. The header of the report displays the total number of alarms to which your operators have responded during the specified time range. (For instructions on specifying the time range, see the topic Setting time range in reports)
4. The report lists all the alarms to which your operators have responded during the specified time range. It also displays the following important parameters for each alarm:
   - **Time to respond** - the time between an alarm being raised and the operator acknowledging it
   - **Time to return** - the time between an alarm being raised and the tag returning to normal
ATTENTION:
This report considers only the alarms that are currently in the CLOSED state. Alarms that are currently OPEN are not displayed.

5. By analyzing operator responses, you can infer the following:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Inference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most operator responses are on output, modes, or set points with cascade masters</td>
<td>Control system problems</td>
</tr>
<tr>
<td>Most operator responses are on set points without supervisory controls</td>
<td>Set points need to be added</td>
</tr>
<tr>
<td>A tag has too many operator responses</td>
<td>The process or limits associated with the tag need to be adjusted</td>
</tr>
<tr>
<td>Operator responses exceed alarm count</td>
<td>Investigation or rationalization is needed</td>
</tr>
</tbody>
</table>

6. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the data that you want to view and analyze</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>Set the time range for the data to be analyzed</td>
<td>Setting time range in reports</td>
</tr>
<tr>
<td>Add comments to the current view</td>
<td>Adding comments to reports</td>
</tr>
<tr>
<td>Export the report to Excel or PDF</td>
<td>Exporting reports to PDF or Excel</td>
</tr>
</tbody>
</table>

4.3 Analyzing chattering alarms

What are chattering alarms?
A tag is considered to contain a chattering alarm if the tag is in alarm two or more times within a specified time window.
For more information about chattering alarms, refer to the topic “About chattering alarms”.
By identifying the chattering alarms in your alarm system and taking necessary actions to prevent them, you can reduce the overload on your operators. The Chattering Alarms report helps you identify bad actors in your alarm system.

To analyze chattering alarms:

1. From any Metrics & Reporting screen, click on the left of the page. The Standard Reports pane appears.

2. Click Chattering Alarms.

   The Chattering Alarms report appears, and displays 5 alarm metrics in one view - Chattering alarms, Fleeting Alarms, Most frequent alarms, Most frequent actions, and Symptomatic report.

3. By default, the Symptomatic Analysis section displays the parent alarms only. To view the child alarms, click .

4. The header of the report displays the percentage contribution of the chattering alarms to your total alarm count.
The above image shows a percentage contribution of 17.24%. In this example, for every 100 alarms generated in your alarm system, 17 were chattering alarms.

5. To analyze the alarms related to a specific tag, click to select that tag in any table/barchart in the report. All the barcharts and tables in the report refresh automatically to highlight (in blue color) the tag you selected. In a single click, you can quickly identify whether a tag that is featured in one of the metrics, is repeated in the other metrics also. This automatic highlighting helps you easily visualize, analyze, and understand the impact of a specific tag on different metrics.

6. You can configure the number of alarms displayed in under Most Frequent Alarms, and the thresholds as follows:

   a. On the top-right corner of the Most Frequent Alarms section, click . The Advanced Settings dialog box appears.
      
      Advanced Settings
      
      Top: 20
      
      Threshold: 1
      
      Information: Chart view will not be available, if number of records returned are more than 30.
      
      Save  Cancel
      
   b. In the Top box, type the number of alarms to be displayed under Most Frequent Alarms.
   c. In the Threshold box, type the threshold limit. Only the alarms whose count exceeds this threshold limit are displayed under Most Frequent Alarms.
      
      Example: If you set the threshold limit to 5, only the alarms that have 5 or more occurrences in the selected time range are displayed.

7. You can select an alarm and click one of the following action icons:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📅</td>
<td>To view the sequence of events related to any shelved or suppressed alarm</td>
</tr>
<tr>
<td>📜</td>
<td>To view the alarm documentation for an alarm</td>
</tr>
</tbody>
</table>
4.4 Assessing standing & stale alarms

Often, a supervisor or an engineer wants to perform a quick assessment of how the plant/area is operating. The Standing & Stale report helps with this task by providing a single view which combines 2 key metrics - the number of standing and stale alarms. It also provides the option to drill down each of these metrics for further understand the situation.

To assess alarms:

1. From any Metrics & Reporting screen, click on the left of the page. The Standard Reports pane appears.
2. Click Standing & Stale. The Standing & Stale report appears and displays the following information:

The section at the top displays the number of Standing and Stale alarms that occurred during the specified time range.

ATTENTION:

The Standing and Stale report displays only those Alarms that were in annunciated state at the end of each time slice. Metrics & Reporting uses the Shelved and Suppressed history to determine if the Alarm was in the annunciated state at that point of time.

- The bar chart represents the standing alarms (default) plotted against time. The data is grouped based on the slicing setting selected with the time range. To view the information related to stale alarms, click the Stale tab.

By default, Standing alarm is selected. In this example, the barchart shows the data for the 7528 Standing alarms.
By default, the last bar in the barchart appears highlighted. The section below the barchart displays the properties of the alarms corresponding to the last bar. Click any bar in the barchart to view the properties of the alarms corresponding to that bar.

To identify whether an alarm is still active, refer to the Is Active column.

To mark an alarm as closed, select the check box in the corresponding row, and click ☑.

3. To view the standing & stale alarms for a specific point in time (and not for a time range), select a single time from the time selection control as shown below:
4. To view the alarm duration column, click the downward arrow at the top-right corner of the table/grid and choose **Columns > Duration (min)**.

5. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the data that you want to view and analyze</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>Set the time range for the data to be analyzed</td>
<td>Setting time range in reports</td>
</tr>
</tbody>
</table>
4.5 Analyzing shelved & suppressed alarms

The Shelved and Suppressed report helps you to analyze the alarms that are suppressed or shelved.

1. From any Metrics & Reporting screen, click on the left of the page.
   The Standard Reports pane appears.
2. Click Shelved and Suppressed.
   The Shelved and Suppressed report appears.

   ![Image of Shelved and Suppressed report](image)

   The tab headers display the count of Shelved alarms and Suppressed tags at the moment you opened the report.
   - The Shelved tab lists the alarms that are shelved by the operator.
   - The Suppressed tab lists the tags that are suppressed (marked as Out of Service).
3. To view the details of the shelved or suppressed alarms, click the appropriate tabs.
   The report displays the tags or conditions (identifiers) that are currently suppressed or shelved. When the tag or condition is suppressed or shelved, the associated alarms are ignored.

   **ATTENTION:**
   For Honeywell Experion DCS, only the disabled (or inhibited) tags are considered as Out of Service (and displayed in the Suppressed tab).

4. By default, the report displays the shelved and suppressed alarms for the current moment only.
   To view the shelved and suppressed data for a past date/time, clear the Active check box at the top-right corner of the screen, and select the time range.

5. The Suppression Category column displays the type of suppression.
   For Honeywell Experion control system:

<table>
<thead>
<tr>
<th>Suppression Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(blank)</td>
<td>A blank value for the suppression category indicates that the tag is explicitly suppressed. This category of suppression is also called out-of-service suppression (OOS). When a tag is suppressed, no Alarms are generated for that tag.</td>
</tr>
</tbody>
</table>
### Suppression Category

<table>
<thead>
<tr>
<th>Suppression Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DAS</td>
<td>Dynamic Alarm Suppression (DAS), also called &quot;Suppression by Design&quot;, prevents the display of an Alarm condition in the operator’s console, based on plant state or condition. <em>Example:</em> A process engineer can configure the control system to automatically suppress a &quot;Pump Flow low&quot; alarm whenever the Pump is not in running state.</td>
</tr>
<tr>
<td>JOURNAL ONLY</td>
<td>This is a special type of suppression where the control system generates events when the Alarm condition becomes true. But, these Process Events are not displayed at the operator's console.</td>
</tr>
</tbody>
</table>

6. You can select one or more alarms (check boxes in the corresponding rows), and click the following action icons:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>⚡</td>
<td>To view the sequence of events related to any shelved or suppressed alarm</td>
</tr>
<tr>
<td>⚡</td>
<td>To remove the suppression for a tag</td>
</tr>
<tr>
<td>⚡</td>
<td>To unshelve an alarm</td>
</tr>
<tr>
<td>⚡</td>
<td>To view the alarm documentation for an alarm</td>
</tr>
</tbody>
</table>

7. You can choose to display only the tags that were suppressed for more than a specific threshold duration.

   To configure the threshold duration:
   
   d. Click ⚡. The **Advanced Settings** dialog box appears.
   
   e. In the **Threshold** box, type the required threshold duration in hours.
   
   f. Click **Save**.

8. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the time range for the data to be analyzed (not applicable if the <strong>Active</strong> check box is selected)</td>
<td>Setting time range in reports</td>
</tr>
<tr>
<td>Filter the data that you want to view and analyze</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>Add comments to the current view</td>
<td>Adding comments to reports</td>
</tr>
</tbody>
</table>

### 4.6 Analyzing operator activity

To analyze the process changes made by your operators, you can use the **Operator Activity** report. The report provides a detailed information which include the list of parameters that were changed, the old and new values of the parameters, the time of change, etc.,

To analyze operator activity:

1. From any Metrics & Reporting screen, click ⚡ on the left of the page.
Analyzing operator activity

The **Standard Reports** pane appears.

2. Click **Operator Activity**.

The **Operator Activity** page appears.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
<th>Parameter</th>
<th>Time</th>
<th>From...</th>
<th>To value</th>
<th>Unit of Measure</th>
<th>Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag24</td>
<td>Parameter0</td>
<td>09 Mar 2017 09:55:01 AM</td>
<td>From371</td>
<td>To7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tag24</td>
<td>Parameter0</td>
<td>09 Mar 2017 09:55:32 AM</td>
<td>From549</td>
<td>To0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tag24</td>
<td>Parameter0</td>
<td>09 Mar 2017 09:52:10 AM</td>
<td>From744</td>
<td>To3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tag24</td>
<td>Parameter0</td>
<td>09 Mar 2017 09:47:40 AM</td>
<td>From570</td>
<td>To6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tag24</td>
<td>Parameter0</td>
<td>09 Mar 2017 09:41:16 AM</td>
<td>From571</td>
<td>To2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tag24</td>
<td>Parameter0</td>
<td>09 Mar 2017 09:40:57 AM</td>
<td>From526</td>
<td>To1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tag24</td>
<td>Parameter0</td>
<td>09 Mar 2017 09:29:21 AM</td>
<td>From222</td>
<td>To7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tag24</td>
<td>Parameter0</td>
<td>09 Mar 2017 09:32:35 AM</td>
<td>From19</td>
<td>To0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tag24</td>
<td>Parameter0</td>
<td>09 Mar 2017 09:31:19 AM</td>
<td>From227</td>
<td>To4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tag24</td>
<td>Parameter0</td>
<td>09 Mar 2017 09:29:55 AM</td>
<td>From995</td>
<td>To5</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the data that you want to view and analyze</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>Set the time range for the data to be analyzed</td>
<td>Setting time range in reports</td>
</tr>
<tr>
<td>Add comments to the current view</td>
<td>Adding comments to reports</td>
</tr>
<tr>
<td>Export the report to Excel or PDF</td>
<td>Exporting reports to PDF or Excel</td>
</tr>
</tbody>
</table>
5. Analyzing & investigating events

5.1 Analyzing & investigating events

Majority of alarms occur due to unforeseen loop-holes in your process. You can identify these alarms and their root causes, and bring in process changes to prevent re-occurrence of such alarms. In other words, you can make continuous improvements to your process, and thereby achieve constant increase in productivity.

The investigation reports of Metrics & Reporting are designed to help with thorough and easy incident investigation, which is a requirement of many industry standards and regulatory bodies.

DynAMo Metrics & Reporting helps in analyzing & investigating alarms in different ways:

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Tools used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyzing action count</td>
<td>Action Count report</td>
</tr>
<tr>
<td>Analyzing the sequence of events</td>
<td>Sequence of Events report</td>
</tr>
<tr>
<td>Analyzing process trends with events</td>
<td>Trending with Events report</td>
</tr>
<tr>
<td>Analyzing alarm interlocks</td>
<td>Interlock Analysis report</td>
</tr>
<tr>
<td>Analyzing alarm count</td>
<td>Alarm Count report</td>
</tr>
<tr>
<td>Analyze alarm distribution</td>
<td>Alarm Distribution report</td>
</tr>
<tr>
<td>Investigating events</td>
<td>Event Investigator report</td>
</tr>
<tr>
<td>Analyzing active alarms</td>
<td>Active Alarms report</td>
</tr>
<tr>
<td>Performing symptomatic analysis</td>
<td>Symptomatic Analysis report</td>
</tr>
</tbody>
</table>

5.2 Analyzing action count

If your operators spend most of their time responding to the same few alarms again and again, then something is wrong. If you get to know which few alarms keep your operators occupied all the time, you can investigate more and find out what is wrong. This analysis helps in identifying control system problems and automation options in your plant. After identifying the root causes the problems, you can resolve them.

The Action Count report helps you analyze the pattern in which your operators respond to alarms.

To analyze action count:

1. From any Metrics & Reporting screen, click on the left of the page.
   The Standard Reports pane appears.
2. Click **Action Count**.
The **Action Count** report appears and displays 2 key alarm metrics:
- **Action Count** - Barchart showing the number of operator plotted actions against time

![Action Count Barchart]

- **Most Frequent Actions** - Barchart showing the top 20 tags responsible for most of the operator actions

![Most Frequent Actions Barchart]

3. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the data that you want to view and analyze</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>Set the time range for the data to be analyzed</td>
<td>Setting time range in reports</td>
</tr>
<tr>
<td>Add comments to the current view</td>
<td>Adding comments to reports</td>
</tr>
<tr>
<td>Export the report to Excel or PDF</td>
<td>Exporting reports to PDF or Excel</td>
</tr>
</tbody>
</table>

### 5.3 Analyzing the sequence of events

**What is "sequence of events"?**
Sequence of events is an event-by-event listing of the alarms and events related to a specific tag.

By analyzing the sequence of events you can:
- identify the root cause of the alarms
- investigate undesirable incidents

The reports of DynAMo Metrics & Reporting allow you to view the sequence of events. The event data is pulled from many event sources and is consolidated and presented as a single list on a common timeline. The events are listed in the sequence of their occurrences. The sequence is so accurate that DynAMo considers even a millisecond-long time difference between events.
By default, **Sequence of Events** report displays up to 1000 records only.

1. From any Metrics & Reporting screen, click  on the left of the page.
   The **Standard Reports** pane appears.

2. Click **Sequence of Events**.
   The **Sequence of Events** report appears.
   The report categorizes the events and presents them under three categories - Alarms, Operator actions, and Others.
   The view uses different symbols to represent the events that belong to different event types. The legend (below the view) shows which symbol represents which event type.

3. To hide the events that belong to a specific event type, click the event type on the legend.
   For example, if you do not want to view the operator actions in the view, click **Alarms** in the legend area of the view. The caption **Alarms** becomes grey and the view refreshes to display the sequence of events excluding the alarms.

   ![Diagram of Sequence of Events](image)

   To unhide (choose not to hide anymore) an event type, click the event type in the legend area again. In the above example, you can unhide the alarms by clicking the **Alarms** in the legend area.
4. The second section of the report lists the tags associated with the events, along with their properties. When you click/select an event in the above plot, the tags associated with the selected event appear highlighted in this list.

5. When you click an alarm / action / other event in the **Sequence of Events** graph, the corresponding row is highlighted in the table. This helps you to quickly view the event details and analyze the events faster.
6. To view additional data fields, clicking the downward arrow in any of the column headers and select the required fields as shown below:

7. To add a comment to one of the rows in the table, select the row and click , type the comment, and click OK.

The comment is added to the row.
8. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the data that you want to view and analyze</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>Set the time range for the data to be analyzed</td>
<td>Setting time range in reports</td>
</tr>
<tr>
<td>Add comments to the current view</td>
<td>Adding comments to reports</td>
</tr>
<tr>
<td>Zoom a specific area in the graphical plot</td>
<td>Zooming the display of trends</td>
</tr>
</tbody>
</table>

5.4 Analyzing process trends with events

If you want to analyze two or more interdependent tags, you need to compare the values recorded for the tags at different points in time. The **Trending with Events** report displays a graphical plot (trend) of the values of a tag over the specified time range, superimposed over the sequence of events for that time range. The report allows you to overlay the graphical trends of up to 8 tags in the same view. This helps in comparing the values of the tags across the time line very easily.

To analyze the process trends with events:

1. From any Metrics & Reporting screen, click on the left of the page. The **Advanced Reports** pane appears.
2. Click **Trending with Events**. The **Trending with Events** report appears.
3. To add tags to the report, click . The **Tag Browser** dialog box appears.
Select the tags that you want to add, and click **OK**.

**ATTENTION:**

When you access this report from a cross-domain instance of Metrics & Reporting, **Tag Browser** is not available. Alternatively, you can add tags using the **Tag Mapping** dialog box (as explained in the next step).

4. In some cases, the historian database (that stores historical data) contains different names for the tags compared to the tag names maintained in the control system.

To map historian tags to the corresponding DCS tags, click ⚗.

The **Tag Mapping** dialog box appears.

To define the mapping:

a. Select each historian tag that you want to map, and type the name of the corresponding event tag.

b. To add a tag mapping, click **Add New**, and type the event tag name and the historian tag name.

c. To view the report based on the tag mappings definitions, click **Apply**.

-OR-

To save the tag mapping definitions and use them whenever you (or other users) open the **Trending with Events** report, then click **Save & Apply**.
5. The second section of the report lists the tags associated with the events, along with their properties. When you click/select an event in the graph, the tags associated with the selected event appear highlighted in this list.

6. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the data that you want to view and analyze</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>Set the time range for the data to be analyzed</td>
<td>Setting time range in reports</td>
</tr>
<tr>
<td>Zoom a specific area in the graphical plot</td>
<td>Zooming the display of trends</td>
</tr>
</tbody>
</table>

5.5 Analyzing alarm interlocks

**What is an interlock?**
In the context of alarm management, the term "interlock" refers to an emergency situation. An interlock can be identified using clearly defined measurable conditions.

Interlock conditions vary from site to site. You can configure the interlock conditions as part of configuring your site. For instructions on configuring interlocks for a site, refer to the *Metrics & Reporting Configuration Guide*.

Typically, the control systems are configured to execute certain special rescue-oriented tasks before and after an emergency situation occurs. These special tasks are called interlock event sequences. After an emergency situation, you might want to analyze whether the interlock sequences executed as configured. The **Interlock Analysis** report allows you to do this.

To analyze alarm interlocks:

1. From any Metrics & Reporting screen, click the Advanced Reports pane appears.

2. Click **Interlock Analysis**.
   The **Interlock Analysis** report appears.

   The event data displayed in the report is automatically filtered based on the interlock conditions.

   **ATTENTION:**
   If the interlock condition returns more than 1000 events, only the first 1000 events are displayed by default. However, you can configure this maximum limit as explained under Configuring Metric Settings in the topic Configuring sites.

3. To view the events that occurred before and after the interlock situation, click to view the **Sequence of Events**. By default, the time range for the sequence of events is defined as per the configured interlock time range.

   **ATTENTION:**
   The **Sequence of Events** report does not take into account very small time differences (millisecond) between the events.

4. In addition, the report allows you to perform the following tasks:
5.6 Analyzing alarm count

A high-level analysis of your alarms and operator actions for a specific time range helps you identify the bad quality alarms. Your analysis is complete if you find answers for the following queries:

- How many alarms were there?
- How loaded were your operator?
- Which are the most frequent alarms?
- Against which alarms were your operators taking actions?
- If no actions were taken against a frequent alarm, is that a bad quality alarm?

The Alarm Count report helps you find answers to these queries. After this high-level analysis, you can drill-down for a deeper analysis using other reports.

To analyze the alarm count:

1. From any Metrics & Reporting screen, click on the left of the page. The Advanced Reports pane appears.
2. Click Alarm Count.

The Alarm Count report appears.
Analyzing alarm distribution

The report displays 3 metrics:

- Alarm count
- Action/Alarms - graphical plot where 3 metrics, plotted against time, are superimposed against one another:
  - Action count (operator responses to alarms)
  - Alarm count
  - Ratio (ratio between action count and alarm count)
- Most frequent alarms - barchart showing the top 20 most frequent alarms

The header of the report displays three statistics:

- Deviation - number of alarms that deviated from the target (based on the alarm rate)
- Average Alarm Count
- Total Alarm Count

3. You can use the following action icons to define how to slice the alarm count for analysis:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To view the alarm count sliced by time</td>
</tr>
<tr>
<td></td>
<td>To view the alarm count sliced by operator positions</td>
</tr>
</tbody>
</table>

4. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the data that you want to view and analyze. This feature allows you to drill down to the tag-level data.</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>Set the time range for the data to be analyzed</td>
<td>Setting time range in reports</td>
</tr>
<tr>
<td>Add comments to the current view</td>
<td>Adding comments to reports</td>
</tr>
<tr>
<td>Export the report to Excel or PDF</td>
<td>Exporting reports to PDF or Excel</td>
</tr>
</tbody>
</table>

5.7 Analyzing alarm distribution

Analyzing alarms requires understanding how your total alarm count is distributed across different days, shifts, priorities, tags, etc. The Alarm Distribution report provides this information readily.

To analyze alarm distribution:

1. From any Metrics & Reporting screen, click on the left of the page.
The **Standard Reports** pane appears.

2. Click **Alarm Distribution**.

   The **Alarm Distribution** report appears and displays the alarm distribution by time (by default).

   ![Alarm Distribution Chart](image)

   3. To view alarm distribution based on another filter, click the corresponding filter in the **Slice By** drop-down list.

   ![Slice By Drop-down List](image)

   **ATTENTION:**
   
   If you have filtered your data based on Operator Positions, you cannot slice by Plant, Area, or Unit. Similarly, if you have filtered your data based on assets, you cannot slice by Operator Position.

   4. To view the alarm distribution using a "group by" condition, click the appropriate filter in the **Group By** drop-down list.

   **ATTENTION:**
   
   **Group By** is supported only where you use **Time** as the **Slice By** filter.
5. Click any item in the legend area to exclude that item in the stacked barchart.
   For example, if you want to exclude TAG20 in the barchart, click TAG20 in the legend area. To
   include the tag in the barchart again, click TAG20 in the legend area again.

6. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the data that you want to view and analyze</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>Set the time range for the data to be analyzed</td>
<td>Setting time range in reports</td>
</tr>
<tr>
<td>Add comments to the current view</td>
<td>Adding comments to reports</td>
</tr>
<tr>
<td>Export the report to Excel or PDF</td>
<td>Exporting reports to PDF or Excel</td>
</tr>
</tbody>
</table>

5.8 Investigating events

If you want to analyze the sequence of events with the ability to filter by alarm parameters, use the Event Investigator reports.

*Example:* You can use this report to identify how many times a tag was suppressed in the past two months. To investigate events:

1. From any Metrics & Reporting screen, click on the left of the page.

   The Advanced Reports pane appears.

2. Click Event Investigator.
The Event Investigator report appears.

<table>
<thead>
<tr>
<th>Time</th>
<th>Tag</th>
<th>Identifier</th>
<th>Priority</th>
<th>Description</th>
<th>Parameter</th>
<th>Path</th>
<th>Operator P...</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 Mar 2017 09:18:57.76 AM</td>
<td>Tag16</td>
<td>Identifier2</td>
<td>Priority2</td>
<td>Parameter0</td>
<td>SampleSite1/Plant0/Area...</td>
<td>OP1</td>
<td></td>
</tr>
<tr>
<td>00 Mar 2017 09:18:57.76 AM</td>
<td>Tag15</td>
<td>Identifier2</td>
<td>Priority2</td>
<td>Parameter0</td>
<td>SampleSite1/Plant0/Area...</td>
<td>OP1</td>
<td></td>
</tr>
<tr>
<td>00 Mar 2017 09:18:24.612 AM</td>
<td>Tag2</td>
<td>Identifier2</td>
<td>Priority2</td>
<td>Parameter0</td>
<td>SampleSite1/Plant0/Area...</td>
<td>OP13</td>
<td></td>
</tr>
<tr>
<td>00 Mar 2017 09:18:24.612 AM</td>
<td>Tag2</td>
<td>Identifier2</td>
<td>Priority2</td>
<td>Parameter0</td>
<td>SampleSite1/Plant0/Area...</td>
<td>OP13</td>
<td></td>
</tr>
<tr>
<td>00 Mar 2017 09:18:14.445 AM</td>
<td>Tag22</td>
<td>Identifier2</td>
<td>Priority2</td>
<td>Parameter0</td>
<td>SampleSite1/Plant0/Area...</td>
<td>OP13</td>
<td></td>
</tr>
<tr>
<td>00 Mar 2017 09:18:09.882 AM</td>
<td>Tag17</td>
<td>Identifier1</td>
<td>Priority1</td>
<td>Parameter0</td>
<td>SampleSite1/Plant0/Area...</td>
<td>OP13</td>
<td></td>
</tr>
<tr>
<td>00 Mar 2017 09:18:09.882 AM</td>
<td>Tag17</td>
<td>Identifier1</td>
<td>Priority1</td>
<td>Parameter0</td>
<td>SampleSite1/Plant0/Area...</td>
<td>OP13</td>
<td></td>
</tr>
<tr>
<td>00 Mar 2017 09:18:02.268 AM</td>
<td>Tag4</td>
<td>Identifier0</td>
<td>Priority0</td>
<td>Parameter0</td>
<td>SampleSite1/Plant0/Area...</td>
<td>OP13</td>
<td></td>
</tr>
</tbody>
</table>

3. To view more data, you can:
   a. Click on the top-right corner of the table. The Columns dialog box appears.
   b. Select the columns that you want to view and close the dialog box.

4. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the time range for the data to be analyzed</td>
<td>Setting time range in reports</td>
</tr>
<tr>
<td>Filter the data that you want to view and analyze</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td></td>
<td>If the selected time range and filtering criteria result in more than 1000 rows of data, the report displays the first 1000 rows only.</td>
</tr>
</tbody>
</table>
5.9 Analyzing active alarms

To view the list of currently active alarms, use the Active Alarms report. The report also highlights whether an alarm is a standing, shelved, or suppressed alarm or a combination of these types.

For some alarms, the visibility is set to false. These alarms do not appear in the operator's console. This report shows these hidden alarms also.

**ATTENTION:**
You cannot use this report to view the alarms that were active during a past time.

To analyze active alarms:

1. From any Metrics & Reporting screen, click on the left of the page. The Advanced Reports pane appears.

2. Click Active Alarms. The Active Alarms page appears.

3. You can select one or more alarms (check boxes in the corresponding rows), and click the following action icons:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔒</td>
<td>To mark an active alarm as closed</td>
</tr>
<tr>
<td>🔵</td>
<td>To view the alarm documentation for an alarm</td>
</tr>
</tbody>
</table>

4. The report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the data that you want to view and analyze</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>Set the time range for the data to be analyzed</td>
<td>Setting time range in reports</td>
</tr>
<tr>
<td>Add comments to the current view</td>
<td>Adding comments to reports</td>
</tr>
<tr>
<td>Export the report to Excel or PDF</td>
<td>Exporting reports to PDF or Excel</td>
</tr>
</tbody>
</table>
5.10 Performing symptomatic analysis

Symptomatic analysis is the process of identifying and eliminating predictable alarms by showing a correlation between the occurrence of an alarm (parent alarm) and the alarms that follow it (child alarms).

The Symptomatic Analysis report helps you to perform symptomatic analysis of alarms.

1. From any Metrics & Reporting screen, click on the left of the page. The Advanced reports pane appears.

2. Click Symptomatic Analysis. The Symptomatic Analysis report appears.

3. By default, the report displays the parent alarms only. To view the child alarms click .

4. You can select one or more alarms (check boxes in the corresponding rows), and click the following action icons:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🕵️‍♂️</td>
<td>To view the sequence of events related to the selected alarm</td>
</tr>
<tr>
<td>📝</td>
<td>To view the alarm documentation for an alarm</td>
</tr>
</tbody>
</table>

5. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the time range for the data to be analyzed (not applicable if the Active check box is selected)</td>
<td>Setting time range in reports</td>
</tr>
<tr>
<td>Filter the data that you want to view and analyze</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>Add comments to the current view</td>
<td>Adding comments to reports</td>
</tr>
<tr>
<td>Export the report to Excel or PDF</td>
<td>Exporting reports to PDF or Excel</td>
</tr>
</tbody>
</table>
6. Resolving alarm issues

6.1 Identifying bad actors

What are bad actors?
Bad actors are the alarms that occur too frequently, and keep your operators always occupied.

By identifying bad actors and taking necessary actions to prevent them, you can reduce the overload on your operators. The **Bad Actor** report helps you identify bad actors in your alarm system.

To identify bad actors:

1. From any Metrics & Reporting screen, click on the left of the page. The **Standard Reports** pane appears.
2. Click **Bad Actors**.
   The **Bad Actors** report appears, and displays 5 alarm metrics in one view - Most frequent alarms, Most frequent actions, Chattering alarms, Fleeting alarms, and Symptomatic analysis.
Identifying bad actors

3. You can configure the number of alarms displayed in under Most Frequent Alarms, and the thresholds as follows:

   c. On the top-right corner of the Most Frequent Alarms section, click 📊. The Advanced Settings dialog box appears.

   Information: Chart view will not be available, if number of records returned are more than 30.

   d. In the Top box, type the number of alarms to be displayed under Most Frequent Alarms.
   e. In the Threshold box, type the threshold limit.

      Only the alarms whose count exceeds this threshold limit are displayed under Most Frequent Alarms.

      Example: If you set the threshold limit to 5, only the alarms that have 5 or more occurrences in the selected time range are displayed.

4. By default, the Symptomatic Analysis section displays the parent alarms only. To view the child alarms click ⬇.

5. The number (highlighted in the image below) on the top-right corner of the report represents the percentage contribution of the top 20 most frequent alarms to your total alarm count.

The above image shows a percentage contribution of 9.22%. In this example, for every 100 alarms generated in your alarm system, 9 were from the top 20 most frequent alarms.
Typically, the top 20 most frequent alarms contribute to more than three-fourths of the total alarm count in a plant. By analyzing these alarms and resolving their root causes, you can bring down your alarm count significantly.

6. To analyze the alarms related to a specific tag, click to select that tag in any table/barchart in the report. All the barcharts and tables in the report refresh automatically to highlight (in blue color) the tag you selected. In a single click, you can quickly identify whether a tag that is featured in one of the metrics, is repeated in the other metrics also. This automatic highlighting helps you easily visualize, analyze, and understand the impact of a specific tag on different metrics.

7. Identify the bad actors and their root causes as explained in the following table:

<table>
<thead>
<tr>
<th>Conditions that indicate a bad actor</th>
<th>Probable root causes</th>
</tr>
</thead>
<tbody>
<tr>
<td>A tag is: listed under &quot;Most frequent alarms&quot; not listed under &quot;Most frequent actions&quot;</td>
<td>Operator is ignoring an alarm that is constantly ringing.</td>
</tr>
<tr>
<td>A tag is: listed under &quot;Most frequent alarms&quot; listed under &quot;Most frequent actions&quot;</td>
<td>Operator is spending a lot of time attending to the same alarm.</td>
</tr>
<tr>
<td>A tag is: listed under &quot;Most frequent alarms&quot; listed under &quot;Chattering alarms&quot;</td>
<td>Review the Sequence of Events (by selecting the tag and clicking 📊) to find the root cause.</td>
</tr>
<tr>
<td>A tag is: listed under &quot;Most frequent alarms&quot; not listed under &quot;Chattering alarms&quot;</td>
<td>Investigate controller problems by removing the alarm, changing the alarm limits, or making the alarm conditional.</td>
</tr>
</tbody>
</table>

8. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the data that you want to view and analyze</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>Set the time range for the data to be analyzed</td>
<td>Setting time range in reports</td>
</tr>
<tr>
<td>Add comments to the current view</td>
<td>Adding comments to reports</td>
</tr>
<tr>
<td>Export the report to Excel or PDF</td>
<td>Exporting reports to PDF or Excel</td>
</tr>
</tbody>
</table>

6.2 Resolving bad actors

A careful analysis of your alarm data can help you find answers to the following queries:

- Are there instrumentation problems in my control system?
- Is there a scope for improvement in my alarm configuration?
- Are there new automation opportunities in my plant?

DynAMo Metrics & Reporting helps you analyze your alarm problems in different ways:
6.3 Analyzing chattering alarms list

What are fleeting alarms?
Fleeting alarm is an alarm that goes ON and, without the operator acting upon it, goes OFF within a short duration. By default, this duration is 5 seconds. Fleeting alarms turn on and off very quickly, but do not necessarily repeat.

You can easily find out the number of chattering & fleeting alarms in your alarm system during a specific time range, using the Chattering Alarms List report.

To analyze chattering and fleeting alarms:

1. From any Metrics & Reporting screen, click on the left of the page.
   The Advanced Reports pane appears.
2. Click Chattering Alarms List.
   The Chattering Alarms List report appears and lists all the chattering alarms that occurred during the specified time range.
3. To view the fleeting alarms, click the **Fleeting Alarms** tab.

![Chattering Alarms Tab Highlighted](image)

<table>
<thead>
<tr>
<th>Fleeting Alarms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td>Tag17</td>
</tr>
<tr>
<td>Tag8</td>
</tr>
<tr>
<td>Tag19</td>
</tr>
<tr>
<td>Tag2</td>
</tr>
<tr>
<td>Tag23</td>
</tr>
</tbody>
</table>

6.4 **Identifying repeat offenders**

To identify the alarms/tags that consistently qualify as bad actors during successive periods of time, use the **Repeat Offenders** report.

**Example:** You can use this report to easily spot an alarm/tag that features in the "Most Frequent Alarms" list week-on-week for the past 1 month.

To identify repeat offenders:

1. From any Metrics & Reporting screen, click on the left of the page.
   The **Advanced Reports** pane appears.

2. Click **Repeat Offenders**.
   The **Repeat Offenders** report appears.

![Repeat Offenders Tab Highlighted](image)

<table>
<thead>
<tr>
<th>Repeat Offenders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td>Tag24</td>
</tr>
<tr>
<td>Tag24</td>
</tr>
<tr>
<td>Tag24</td>
</tr>
<tr>
<td>Tag24</td>
</tr>
<tr>
<td>Tag24</td>
</tr>
<tr>
<td>Tag24</td>
</tr>
<tr>
<td>Tag24</td>
</tr>
</tbody>
</table>

3. To view the alarm documentation for an alarm, click (to select) the corresponding row and then click .

4. You can configure the number of alarms to be considered for deriving the "Most Frequent Alarms" list, and the thresholds as follows:
a. On the top-right corner of the report, click 

The Advanced Settings dialog box appears.

**Advanced Settings**

<table>
<thead>
<tr>
<th>Top:</th>
<th>20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threshold</td>
<td>1</td>
</tr>
</tbody>
</table>

b. In the **Top** box, type the number of alarms to be considered for deriving the "Most Frequent Alarms" list.

c. In the **Threshold** box, type the threshold limit.

Only the alarms whose count exceeds this threshold limit are considered as "Most Frequent Alarms".

**Example:** If you set the threshold limit to 5, only the alarms that have 5 or more occurrences in the selected time range are considered as "Most Frequent Alarms" for that time range.

5. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the time range for the data to be</td>
<td>Setting time range in reports</td>
</tr>
<tr>
<td>analyzed</td>
<td></td>
</tr>
<tr>
<td>Filter the data that you want to view</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>and analyze</td>
<td></td>
</tr>
<tr>
<td>Add comments to the current view</td>
<td>Adding comments to reports</td>
</tr>
</tbody>
</table>

### 6.5 Analyzing alarm floods

**What is alarm flood?**

An alarm flood starts when an operator receives >9 alarms within a 10-minute interval.

The flood ends on encountering a 10-minute interval where the operator receives <5 alarms.

Typically, an operator can manage to handle up to 9 alarms during a 10-minute interval. But, if this continues to happen during two or more successive 10-minute intervals, it becomes very difficult to handle.
To ensure that your operators are loaded reasonably, you must regularly analyze your alarms and operator actions over a time range and find answers to the following queries:

- Was there an alarm flood?
- What proportion of the specified time range was under flood?
- How many floods occur?
- What was the peak alarm rate during each flood?
- Are these floods interrelated? (Do have parent-child relationship?)
- How many actions did my operators perform versus the number of alarms?
- If my operators did not take any action against a most frequent alarm, is that a bad quality alarm?

To analyze the alarm flood:

1. From any Metrics & Reporting screen, click on the left of the page. The **Standard Reports** pane appears.
2. Click **Alarm Flood**. The **Alarm Flood** smart view appears.

   ![](image)

   The report displays 3 metrics:
   
   - Alarm count
   - Action/Alarms - graphical plot where 3 metrics, plotted against time, are superimposed against one another:
     - Action count (operator responses to alarms)
     - Alarm count
     - Ratio (ratio between action count and alarm count)
   - Symptomatic analysis - An analysis of the predictability and significance of assuming a parent-child relationship between alarms. See the topic **Symptomatic analysis** for details.

3. By default, the **Symptomatic Analysis** section displays the parent alarms only. To view the child alarms, click .
The header displays 2 metrics:

- Number of floods
- Number of operator positions where flood occurred

5. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the data that you want to view</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>and analyze</td>
<td></td>
</tr>
<tr>
<td>Set the time range for the data to be</td>
<td>Setting time range in reports</td>
</tr>
<tr>
<td>analyzed</td>
<td></td>
</tr>
<tr>
<td>Add comments to the current view</td>
<td>Adding comments to reports</td>
</tr>
<tr>
<td>Export the report to Excel or PDF</td>
<td>Exporting reports to PDF or Excel</td>
</tr>
<tr>
<td>Zoom a specific area in the graphical</td>
<td>Zooming the display of trends</td>
</tr>
<tr>
<td>plot</td>
<td></td>
</tr>
</tbody>
</table>
7. Viewing Documentation & Enforcement data

7.1 Overview

If you have configured the connection to the Documentation & Enforcement (D&E) application and mapped the Operator Positions against the D&E Consoles, you can view and analyze D&E data in Metrics & Reporting. For instructions on configuration D&E connection, refer to the DynAMo Metrics & Reporting Configuration Guide.

Metrics & Reporting allows you to perform the following tasks with D&E data:

- View D&E Enforcements
- Investigate D&E Enforcements
- Analyze D&E alarm priorities
- Identify D&E unmanaged tags

7.2 Viewing D&E Enforcements

This report is applicable only if you are using the DynAMo Documentation & Enforcement application. If you need to review the enforcement sessions at a high level, use the D&E Enforcement Summary report.

1. From any Metrics & Reporting screen, click the Advanced Reports button on the left of the page.
   The Advanced Reports pane appears.
2. Click D&E Enforcement Summary.
   The D&E Enforcement Summary report appears.

The report displays a high-level summary of all the enforcement sessions that occurred during the specified time range.

3. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the data that you want to view and analyze</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>Set the time range for the data to be analyzed</td>
<td>Setting time range in reports</td>
</tr>
<tr>
<td>Add comments to the current view</td>
<td>Adding comments to reports</td>
</tr>
<tr>
<td>Export the report to Excel or PDF</td>
<td>Exporting reports to PDF or Excel</td>
</tr>
</tbody>
</table>

7.3 Investigating D&E Enforcements

This report is applicable only if you are using the DynAMo Documentation & Enforcement application. If you need to investigate each enforcement session in detail, use the D&E Enforcement Details report.

1. From any Metrics & Reporting screen, click the Advanced Reports button on the left of the page.
   The Advanced Reports pane appears.
2. Click **D&E Enforcement Details**.

The **D&E Enforcement Details** report appears.

The **Consoles** list displays all the consoles configured in Documentation & Enforcement.

3. To investigate enforcements associated with a console, click that console in the **Consoles** list.

The **Sessions** table lists the enforcement sessions associated with the selected console.

4. To view tag-level details for a specific enforcement session, click the corresponding row in the **Sessions** table.

The **Session Details** table lists all the tag-level enforcements that occurred during the session.

5. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the data that you want to view and analyze</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>Set the time range for the data to be analyzed</td>
<td>Setting time range in reports</td>
</tr>
<tr>
<td>Add comments to the current view</td>
<td>Adding comments to reports</td>
</tr>
<tr>
<td>Export the report to Excel or PDF</td>
<td>Exporting reports to PDF or Excel</td>
</tr>
</tbody>
</table>

### 7.4 Analyzing D&E alarm priorities

This report is applicable only if you are using the DynAMo Documentation & Enforcement application.

If you need to analyze how your alarms are distributed based on the priorities defined in the Documentation & Enforcement application, use the **D&E Alarm Priorities** report.

To analyze the distribution of alarms based on priorities:

1. From any Metrics & Reporting screen, click ![Advanced](image) on the left of the page.

The **Advanced Reports** pane appears.

2. Click **D&E Alarms Priority Distribution**.

The **D&E Alarms Priority Distribution** report appears.
The report displays a pie chart that shows how your alarms are distributed based on their priorities.

**ATTENTION:**

- The data in this report is applicable for the base mode (in D&E) only.
- Using this report, you can analyze the alarm priority distribution for event data from up to 8 D&E consoles. If you attempt to view data from more than 8 consoles, then the report shows the data from 8 consoles only. No error or warning message is displayed. (You can configure this limit by modifying the \texttt{MaxConsoleCount} parameter.)

3. Click a priority type in the legend area to view the pie chart again without that priority type.

For example, if you do not want to view "Critical" alarms in the pie chart, click "Critical" in the legend area. To include the "Critical" priority alarms in the pie chart again, click "Critical" in the legend area again.

4. The table displays the percentage distribution for each priority and the number of alarms under each priority type for each of the selected consoles.

5. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the data that you want to view and analyze</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>Set the time range for the data to be analyzed</td>
<td>Setting time range in reports</td>
</tr>
<tr>
<td>Add comments to the current view</td>
<td>Adding comments to reports</td>
</tr>
<tr>
<td>Export the report to Excel or PDF</td>
<td>Exporting reports to PDF or Excel</td>
</tr>
</tbody>
</table>
### 7.5 Identifying D&E unmanaged tags

This report is applicable only if you are using the DynAMo Documentation & Enforcement application. In a plant it is sometimes possible that the event data collected by the Metrics & Reporting application contains unknown tags that are not managed in the Documentation & Enforcement application. You can identify such tags using the **D&E Unmanaged Tags** report.

To identify D&E unmanaged tags:

1. From any Metrics & Reporting screen, click on the left of the page. The **Advanced Reports** pane appears.
2. Click **D&E Unmanaged Tags**.
   - The **D&E Unmanaged Tags** report appears.

   ![D&E Unmanaged Tags Report](image)

   The report lists the unmanaged tags grouped by Operator Positions, and then by assets.

   3. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter the data that you want to view and analyze</td>
<td>Filtering data in reports</td>
</tr>
<tr>
<td>Add comments to the current view</td>
<td>Adding comments to reports</td>
</tr>
<tr>
<td>Export the report to Excel or PDF</td>
<td>Exporting reports to PDF or Excel</td>
</tr>
</tbody>
</table>
8. Viewing real-time messages

8.1 Viewing real-time events

To perform real-time monitoring of event data, use the **Real-time Events Viewer** report. The report receives live alarm messages from the DynAMo M&R Archiver.

To monitor real-time alarm data:

1. From any Metrics & Reporting screen, click on the left of the page.
   The **Advanced Reports** pane appears.

2. Click **Real-time Events Viewer**.
   The **Real-time Events Viewer** report appears.

   ![Real-time Events Viewer](image)

   The report displays live events as they are received from the control system. If the number of rows exceeds 100 (you can configure this duration by modifying the **EventsMaxRows** parameter), the oldest event is removed from the grid whenever a new event arrives.

3. The or icon indicates whether the connection is alive, and new event messages are being received.

4. Use the following action icons as required:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>To view the alarm documentation for an alarm</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>To view the sequence of events related to the selected tag for the last 24 hours</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>To refresh the list of messages displayed. When you refresh the</td>
</tr>
</tbody>
</table>

5. To pause live event monitoring, click or select any row in the grid.

   All the event messages, that are newly collected while live monitoring is paused, are not displayed in the grid.

   Live alarm monitoring automatically resumes after 30 seconds (you can configure this duration by modifying the **PauseTimeout** parameter). When you move your mouse over the icon, a tool tip appears and displays the number of seconds left before the automatic resume occurs.
To manually resume live event monitoring, click 🔄.

6. You can configure conditional formatting that enables Metrics & Reporting to automatically highlight a message with a background color and icon if the message conforms to the specified condition(s). To configure conditional formatting:

   a. Click Formats at the top-right corner of the screen. The Formats dialog box appears.
   b. In the Enter format name box, type a name for the conditional formatting and click +. A new conditional formatting entry is created.
   c. From the Color drop-down list, select the required background color for highlighting the message text.
   d. From the Icon drop-down list, select an icon for the message text.
   e. Use the options under Conditions, to form conditional expressions and click +. Similarly, add as many conditions as required.
   f. Click Save. All event messages that conform to the above conditions appear highlighted with the specified color and icon.

7. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add comments to the current view</td>
<td>[Adding comments to reports]</td>
</tr>
<tr>
<td>Export the report to Excel</td>
<td>[Exporting reports to PDF or Excel] (Exporting to PDF is not available for this report)</td>
</tr>
</tbody>
</table>
8. You can filter the data in the report as explained in the topic Filtering data in reports, but with the following exceptions:

- You can filter the data by channels also.
- The Filters pane provides the options to filter the data by assets, operator positions, and channels. To filter by other fields, click Advanced Filters and add the filtering criteria in the pop-up window that appears. After adding the filtering criteria, close the Advanced Filters dialog box and click on the Filters pane to apply the filter.

8.2 Viewing real-time alarms

To perform real-time monitoring of alarm data, use the Real-time Alarms Viewer report. The report receives live alarm messages from the DynAMo M&R Archiver.

To monitor real-time alarm data:

1. From any Metrics & Reporting screen, click on the left of the page.
   The Advanced Reports pane appears.

2. Click Real-time Alarms Viewer.
   The Real-time Alarms Viewer report appears.
Viewing real-time alarms

The report displays live alarm messages as they are received from the control system. If the number of rows exceeds 100 (you can configure this duration by modifying the `AlarmsMaxRows` parameter), the oldest alarm is removed from the grid whenever a new alarm arrives.

On receiving an ACKNOWLEDGE event for an alarm, the value in the `Message Type` column changes to "Acknowledge". Also, the `Time` column is updated with the time of receipt of the ACKNOWLEDGE event.

**TIP:**
You can create formatting rules (explained later in this procedure) to easily differentiate acknowledged alarms from the non-acknowledged alarms.

**ATTENTION:**
Each alarm displayed in the report is automatically removed from the grid when a corresponding RETURN message is received.

3. The или icon indicates whether the connection is alive, and new event messages are being received.

4. To view the alarm help for any of the tags listed, click the tag name in the `Tag` column.

5. If you need to sort and analyze the alarm messages, click .

The screen splits into two horizontal halves, and displays two grids:

- **Lower grid** - All the alarm messages that were displayed in the report are now moved to the lower grid and sorted by time in the descending order. To sort by ascending order, click the column header of the `Time` column again. To sort by any other column, click the corresponding column header.

- **Upper grid** - All new incoming alarm messages appear in the upper grid.

**ATTENTION:**
Similar to the upper grid, alarms listed in the lower grid are also removed on receiving the corresponding RETURN messages.
After you finish analyzing the sorted event messages, click to close the lower grid.

6. Use the following action icons as required:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
</table>
|       | To remove all messages from the grid  
New messages continue to get added to the grid as they are received. |
|       | To view the alarm properties for the selected tag |
|       | To remove an alarm from the grid |
|       | To view the sequence of events related to the selected tag for the last 24 hours (in a new browser window) |

7. To pause live alarm monitoring, click or select any row in the grid.

All the alarm messages, that are newly collected while live monitoring is paused, are not displayed in the grid.

Live alarm monitoring automatically resumes after 30 seconds (you can configure this duration by modifying the PauseTimeout parameter). When you move your mouse over the icon, a tool tip appears and displays the number of seconds left before the automatic resume occurs.
To manually resume live alarm monitoring, click 

8. You can configure conditional formatting that enables Metrics & Reporting to automatically highlight a message with a background color and icon if the message conforms to the specified condition(s). To configure conditional formatting:

   a. Click  at the top-right corner of the screen. The Formats dialog box appears.
   b. In the Enter format name box, type a name for the conditional formatting and click +. A new conditional formatting entry is created.
   c. From the Color drop-down list, select the required background color for highlighting the message text.
   d. From the Icon drop-down list, select an icon for the message text.
   e. Use the options under Conditions, to form conditional expressions and click +. Similarly, add as many conditions as required.
   f. Click Save. All event messages that conform to the above conditions appear highlighted with the specified color and icon.

9. In addition, the report allows you to perform the following tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>Reference topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add comments to the current view</td>
<td>Adding comments to reports</td>
</tr>
<tr>
<td>Export the report to Excel</td>
<td>Exporting reports to PDF or Excel</td>
</tr>
<tr>
<td></td>
<td>(Exporting to PDF is not available for this report)</td>
</tr>
</tbody>
</table>


9. Reference topics

9.1 About symptomatic analysis

Overview

Symptomatic analysis is the process of identifying and eliminating predictable alarms by showing a correlation between the occurrence of an alarm (parent alarm) and the alarms that follow it (child alarms). Symptomatic analysis helps you in calculating the following parameters:

- **Predictability** - The probability to predict that if a parent alarm occurs, one of its child alarms will follow immediately (within a configured time window).
- **Significance** - The probability to infer that when a child alarm occurs, its parent alarm has occurred recently (within a configured time window).

Where predictability is more than 50%, you can suppress (exclude from reports) the child alarms. This reduces the number of alarms displayed on the console thereby reducing operators' workload.

A cutout occurs when an alarm treats another tag as permissive. That is, when one alarm also contains the conditions set in another. A cutout would remove one alarm if the other alarm is in. Before adding a cutout, it is important to ensure that the child alarm does not indicate another condition.

An illustration for symptomatic analysis

This example illustrates symptomatic analysis for an alarm system with the following settings:

*Time range: 10 minutes*

*Time window: 1 minute*

*Count threshold: 2*
About symptomatic analysis

**Analysis**
During the 10-minute time range, Tag A alarms occurred 5 times, and Tag B alarms occurred 4 times.

All 4 occurrences of Tag B alarms were:
- preceded by Tag A alarms
- within 1 minute (configured time window) after Tag A alarms

**Results**
From the above analysis, we can infer that Tag B alarm is a child alarm for Tag A alarm. The results of the symptomatic analysis (Predictability and Significance) are calculated as follows:

**Predictability**
In this example, predictability is the probability of a Tag B alarm to occur within 1 minute of the occurrence of a Tag A alarm.

\[
\text{Predictability} = \left( \frac{\text{No of occurrences of Tag A alarm where Tag B alarm occurred within the next 1 minute}}{\text{Total no of occurrences of Tag A alarm}} \right) \times 100
\]

\[
= \left( \frac{4}{5} \right) \times 100
\]

\[= 80\%
\]

**Significance**
In this example, significance is the probability of a Tag A alarm to have occurred 1 minute prior to a Tag B alarm.

\[
\text{Significance} = \left( \frac{\text{No of times a Tag B alarm occurred within 1 min of Tag A alarm}}{\text{Total no of occurrences of Tag B alarm}} \right) \times 100
\]

\[
= \left( \frac{4}{4} \right) \times 100
\]

\[= 100\%
\]

**Impact of Count Threshold**
In this example, the parent-child pairing occurs 4 times in the given 10-minute time range. Since this number (4) is more than the Count threshold (2) that you have configured, the observations are taken into consideration for the symptomatic analysis.
If you had configured the Count threshold as 5, you do not have enough number of occurrences of parent-child pairing in the given time window. So, you could not have performed symptomatic analysis on the given sample data.

9.2 Standing and stale alarms

**ATTENTION:**
The standing alarm and stale alarm duration metrics displayed in the reports do not take into account, the shelved/suppressed duration and status of an alarm, if the alarm was:
- shelved and later closed via DCS or by the Operator
- shelved and unshelved within the standing alarm duration

**Standing alarms**
Standing alarm is an alarm whose alarm condition is true.

**Stale alarms**
Stale alarms are alarms whose alarm conditions remain true for more than 24 hrs.
Standards suggest that the stale alarm count should not exceed 5 alarms per day per console.

**ATTENTION:**
You can configure the stale alarm duration as part of site configuration.

9.3 Chattering and fleeting alarms

**Chattering Alarms**
A tag is considered to contain a chattering alarm if the tag is in alarm two or more times within a specified time window.

Chattering alarms cause noise in an alarm system. Since an operator’s attention is needlessly interrupted by these nuisance alarms, they are a major contributor to operator overload. It is very essential that you identify and eliminate chattering alarms to ensure that your operators spend their time effectively.

Chattering alarms can occur due to many reasons:
- Control loops cycling repeatedly
- A noisy process variable at a value near the alarm setting
- Real process variability at a value near the alarm setting

A *cluster* is a group of alarms that repeats within the specified cluster time and in subsequent continuous windows. The time window is a time in seconds that defines what DynAMo M&R considers a cluster.
DynAMo Metrics & Reporting identifies chattering alarms by looking for recurring alarms within the time window, and for subsequent occurrences of the same alarm in adjacent time windows. Alarms in the time period that repeat within these windows are members of a chattering cluster. A window with one alarm occurrence only, that is, the initial alarm at the window’s leading edge, constitutes a break in the cluster.

An alarm flood starts when an operator receives >9 alarms within a 10-minute period, and ends when the operator receives <5 alarms in a 10-minute period.

**ATTENTION:**

As part of site configuration, you can configure the time window, and the number of occurrences for an alarm to qualify as a chattering alarm.

To understand the parameters of a chattering alarm, consider the following scenario where the time window is set to 15 seconds.

Following are the parameters for analyzing the chattering alarms for a specific tag during a specific time range:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total occurrences</td>
<td>In the above illustration, the alarm occurred 11 times during the 1-minute time range.</td>
</tr>
<tr>
<td>Number of clusters</td>
<td>There were 3 clusters in the above illustration.</td>
</tr>
</tbody>
</table>
### Advanced configuration settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Average number of cluster members | The 3 clusters in the above illustration had 3, 4, and 3 occurrences of the alarm respectively. So, average number of cluster members  
= \( \frac{3 + 4 + 3}{3} \)  
= 10/3  
= 3.33 |
| Cluster member percentage         | The ratio between "the occurrences of the tag in clusters" and "total occurrences of the tag"  
In the above illustration, cluster member percentage  
= \( \frac{3 + 4 + 3}{3 + 4 + 1 + 3} \)  
= 10/11  
= 0.91 |
| Alarm count from chatter          | The number of occurrences of the tag in clusters  
In the above illustration, alarm count from chatter  
= 3 + 4 + 3  
= 10 |

When the alarm chattered in two or more consecutive 15-second periods, a cluster was formed. The 15-second time window, where the alarm did not chatter, is not part of any cluster.

**Fleeting alarms**

Fleeting alarm is an alarm that goes ON and, without the operator acting upon it, goes OFF within a short duration. By default, this duration is 5 seconds. Fleeting alarms turn on and off very quickly, but do not necessarily repeat.

**ATTENTION:**

As part of site configuration, you can configure the maximum duration the alarm should stay ON, to qualify as a fleeting alarm.