FT Analytics™ GuardianAI™

User Guide

Version 1.03.00

Rockwell Automation Publication FTGAI 95055-UM012E-EN-P

Rockwell Automation

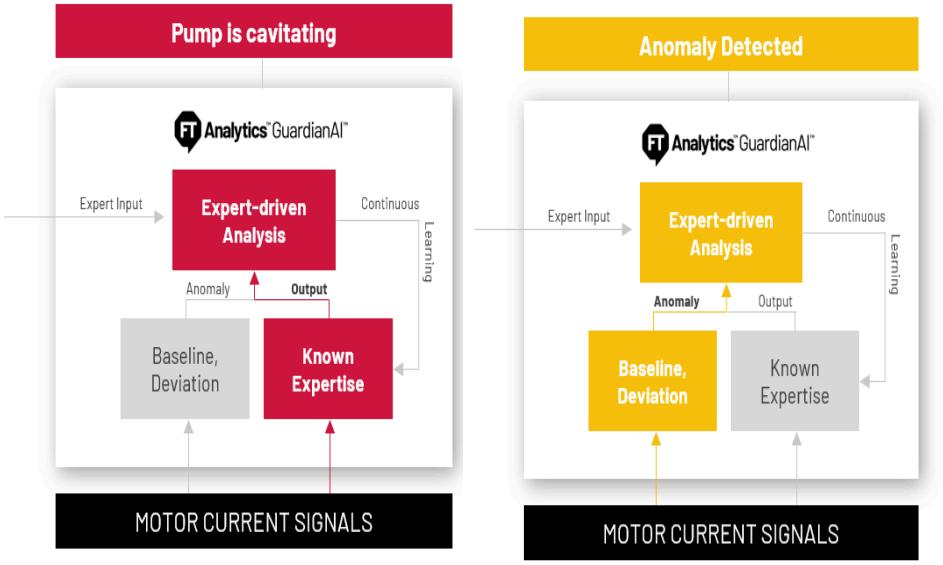
Original Instructions

Contents

This page has been intentionally left blank

FactoryTalk Analytics GuardianAI Overview

FactoryTalk® Analytics™ GuardianAI™ (hereafter called as GuardianAI) is a machine learning based supervisory application that uses existing plant devices, such as variable-frequency drives, as sensors to monitor the health of components such as pumps, fans, and blowers on a plant floor. It uses device data to establish a baseline signature of each component's behavior under normal operating conditions. Then, it monitors the components for any deviation from the baseline. Once a deviation is detected, a notification is sent to the user identifying the anomaly. If an anomaly is detected but cannot be identified, GuardianAI notifies the maintenance engineer that an unidentified anomaly was detected. The engineer can then investigate the issue, determine the cause of the anomaly, and tag the deviation accordingly. The machine learning engine in GuardianAI then trains to identify new anomalies for future encounters. The following diagram illustrates this process and the variation between a known fault and an unknown deviation.



The GuardianAI workflow takes a no-code approach to machine learning. As a result, a data scientist is not required to configure, deploy, or use this AI application. It is designed so that OT personnel, such as maintenance engineers, controls engineers, machine operators, and plant managers, can work with GuardianAI with minimal training required.

The configuration workflow consists of four steps.

1. Deploy the GuardianAI application on a local Virtual Machine.
2. Add the device that will act as a sensor.
3. Provide the identifying information about the component being monitored (pump, fan, blower, or motor).
4. Training the model to establish the baseline.

GuardianAI supports monitoring multiple baselines based on a component's state. Components such as pumps, motors, fans, and blowers on a plant floor can operate under different conditions and processes. GuardianAI provides the capability to monitor these varying situations.

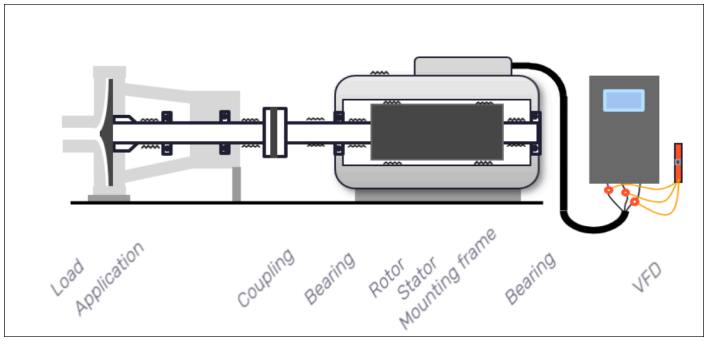
NOTE: State refers to a component's specific operating condition, such as different pressures, flow rates, speed, etc.

GuardianAI provides premium integration with the controller to seamlessly read changes in the component's tags selected during configuration. When a component's tag value in the controller changes, GuardianAI automatically creates a new state and starts acquiring the baseline for that specific state. Once the baseline is acquired, GuardianAI continuously monitors the component for any deviation in that particular state. GuardianAI will automatically switch to the corresponding state based on the change in the controller tags to ensure accurate monitoring.

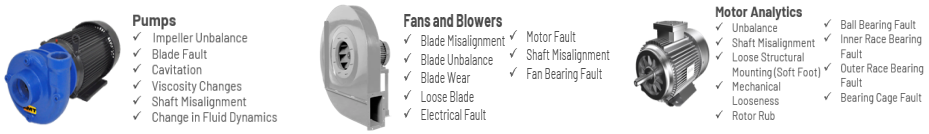
For example, if a pump operates under different pressures or flow rates, GuardianAI will create and monitor baselines for each condition and switch to the appropriate state when the component's operating condition changes to ensure accurate monitoring.

GuardianAI provides premier integration with PowerFlex® 755, 755TL, 755TR, 755HiHP, 755TM, 755TS, and 6000T drives to use as sensors to access three-phase current data for motor current signature analysis. It focuses on anomaly detection and identification for the following component types: pumps, fans, and blowers. The application is designed to work with single-drive and motor applications. Given its adaptive nature, GuardianAI can learn process-centric issues and adapt to asset types beyond those listed above. For this use case, the application comes equipped with generic motor control analytics.

Figure 1. Example of a VFD connected to a motor with direct coupling to a Component



Beyond the classification provided by the maintenance engineers, GuardianAI comes equipped with embedded expertise to detect certain anomaly patterns that are out of the box, as outlined below.



Key Features

- **No Code** GuardianAI provides no code machine learning. It puts AI into the hands of OT professionals without the need for data science experience.
- **Existing Devices Act as Sensors** Users do not need to purchase additional equipment or sensors to get predictive maintenance insights. Early warnings of potential equipment failures are provided leveraging data already available on the plant floor.
- **Anomaly Identification** GuardianAI goes beyond anomaly detection. It provides users with context about what type of failure will occur which reduces investigation time and reduces maintenance costs and plant downtime.

- **At the Edge** There is no need to send large quantities of raw data to the cloud for analysis. GuardianAI trains and runs right at the edge providing real-time predictions and minimizing the total cost of ownership.
- **Controller Connection** To read the tags and define the states of the component operation.
- **Multiple Baselines** GuardianAI supports monitoring multiple baselines of a component based on its state value coming from the PLC.

This page has been intentionally left blank

Getting Started with FactoryTalk Analytics GuardianAI

The GuardianAI user experience has four main workspaces: Monitoring, Single Asset View, Configuration, and System Setting.

User Interface

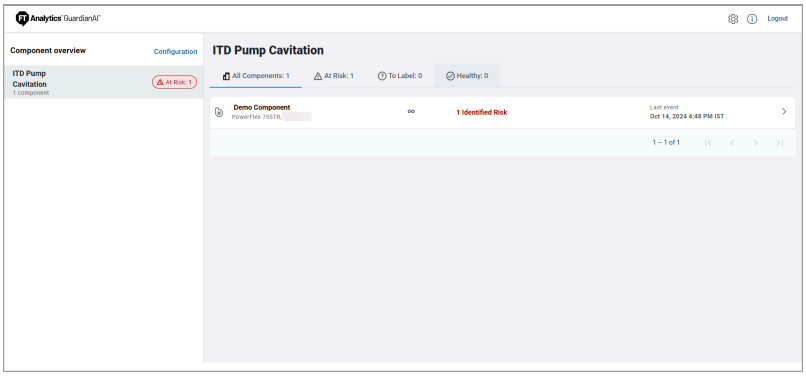
This topic will help you get familiar with the GuardianAI user interface.

Monitoring Workspace

The monitoring workspace, displayed in the following figure, provides quick access to the overall status of the components monitored by GuardianAI.

1. The left panel displays the different folders containing the component.
    - When a component in a folder encounters a deviation or failure risk, a tag on the folder illustrates the count of components encountering those events.
2. The quick filters allow the user to gain additional insight into the components with a failure risk, deviation requiring labeling, or healthy components (no action required). Upon selecting a filter, only the components meeting the criteria are displayed.
3. The detailed component page displays all information about the component, including a detailed view of deviations or failure risks requiring user action.

Figure 2. Component Monitoring Workspace



Single Component View

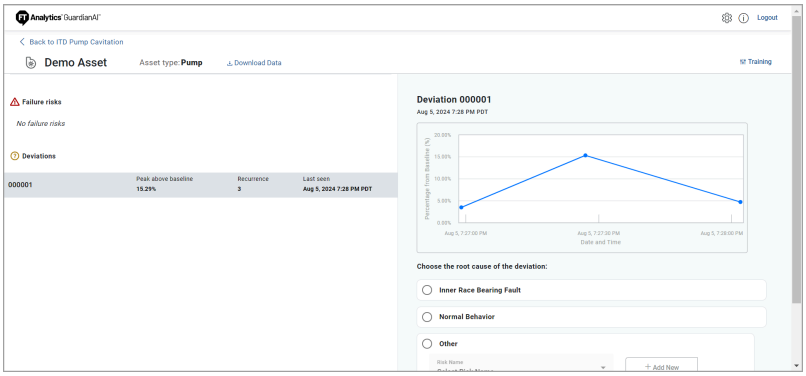
The single component page provides detailed insight regarding deviations and failure risks encountered while monitoring. All new anomalies are displayed as deviations until a user labels the item. Once labeled, a deviation becomes a failure risk.

A failure risk is a previously encountered deviation labeled and confirmed by a user.

The following image displays a deviation. If the component is having multiple states, the deviation and failure risk information particular to current active state will be displayed. Once displayed, the deviation will have a set of first principle recommendations for the user to select from. GuardianAI detected a deviation with a signature matching pump cavitation or a fluid viscosity change in the following example. If the user believes the deviation is incorrect, they can select normal operation or create a new label.

Users can download the raw data of training, deviation, and failure risk of the drive to analyze the data.

Figure 3. Single Asset View with Deviation Detected

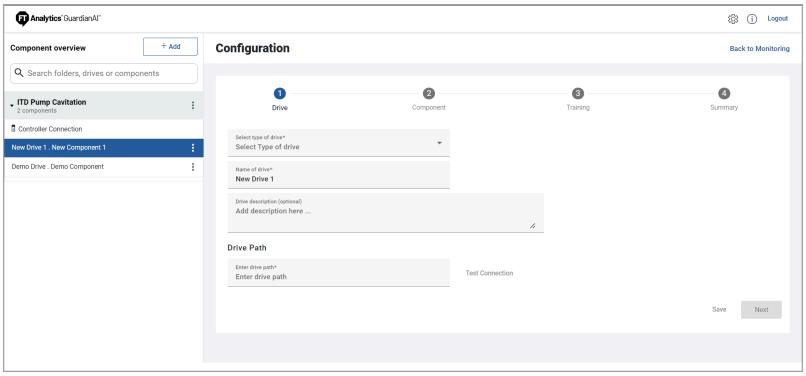


Configuration Workspace

The configuration workspace, accessible from the monitoring workspace, is where users can create folders, add drives, define the component the drive is powering, and configure the training parameters. The workflow is designed with an easy-to-use stepper to guide the user in creating a new component for GuardianAI to monitor.

Additionally, controller configuration is available for each folder to read the tags seamlessly and monitor multiple states of the component based on the state value coming from the PLC. The controller configuration is optional.

Figure 4. Configuration Workspace to Add a New Component

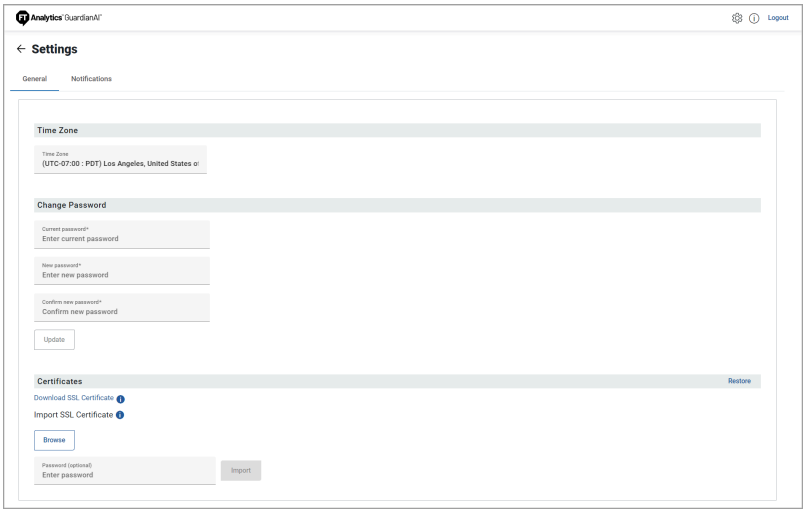


System Settings Workspace

The Settings workspace allows the user to control additional GuardianAI parameters.

- **Timezone**: Timezones are used to display the timestamps for detected deviations and failure risk events. Rockwell Automation recommends that the timezone must match the physical location of the compute surface used to host GuardianAI.
- **Change Password**: Users can modify their password to access the application.
- **Certificates**: Certificates are used to establish the webpage identity for GuardianAI. The application comes out of the box with a self-signed certificate. Users have the option to upload their certificates.

Figure 5. System Settings - Application Parameters Configuration

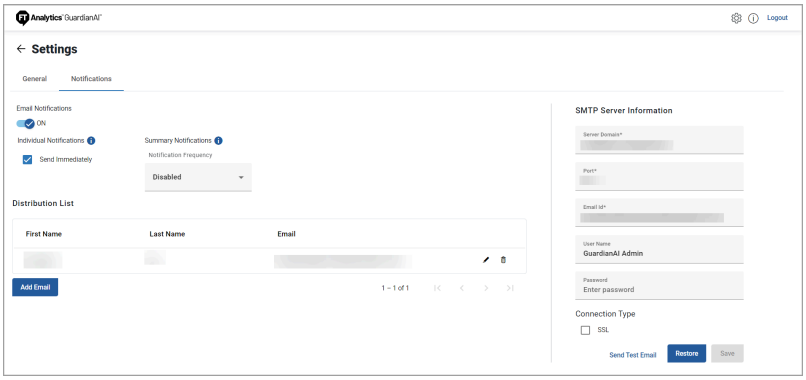


Notifications

The notification settings enable GuardianAI to connect to an SMTP server to send notifications when a deviation or failure risk event has been detected. The Notifications workspace includes:

- Ability to turn notifications on or off.
- SMTP Server Information
- Mailing list configuration to add and remove recipients.

Figure 6. System Setting - Email Notification Configuration



Variable Frequency Drive Prerequisites and Considerations

High-Speed Trend Configuration

- GuardianAI utilizes the high-speed trend function of the variable frequency drives. This function will not be available for other application usage while GuardianAI is training and monitoring the component. A user should stop training and monitoring with GuardianAI to release usage of the High-Speed data trend.
- The data is collected for a period of 4 seconds at 1 msec increment, so 4K of data is collected in a single buffer. During that period, the frequency must be within the 1/2 Hz range for each entry in the 4K buffer; otherwise, when delivered to GuardianAI, it will be rejected.
- Usage of the high-speed data trend by other applications while GuardianAI is training and monitoring a component may impact GuardianAI's performance in creating a baseline and detecting deviations.

FactoryTalk Analytics GuardianAI utilizes test point parameters to perform its high-speed trending. While FactoryTalk Analytics GuardianAI is performing training or monitoring with a drive, the following test point parameters will be unavailable for other application usage:

- PowerFlex 755T and 6000T
  - [10:0381] Testpoint REAL 1
  - [10:0384] Testpoint REAL 2
  - [10:0387] Testpoint REAL 3
- PowerFlex 755
  - [00:0971] Testpoint Fval 1
  - [00:0975] Testpoint Fval 2
  - [00:0979] Testpoint Fval 3

Drive Firmware Version Support

- PowerFlex 755 firmware version 16 is not supported by GuardianAI.

Configuring Controller

GuardianAI allows the user to configure a controller to read the tags and monitor multiple component baselines based on the state value read from the PLC. This configuration is optional.

Perform the following steps to configure a controller in GuardianAI:

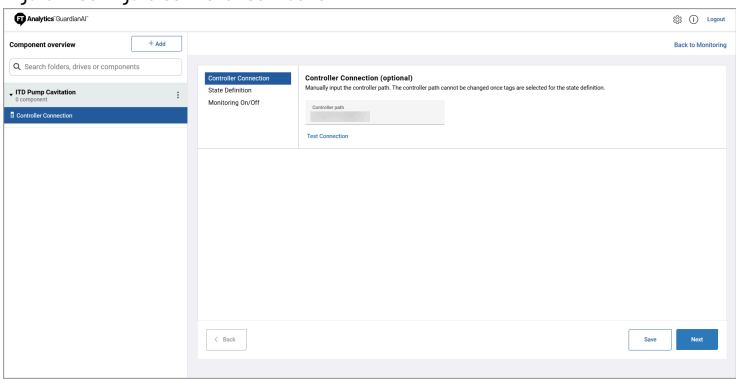
1. On the **Component overview** section, click **Configuration**.
2. On the **Controller Connection** page, provide the **Controller path**.

   Following is an example format for the controller path: *:<Ethernet bridge IP address>/<Chassis port>:<Slot>

   Example controller path: **2:192.168.1.0/1:0**

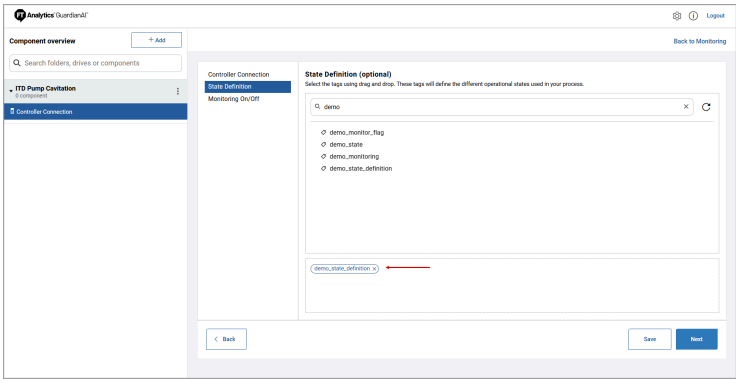
   Following is an example where the user can access the controller in chassis 2 from the workstation: **2:192.168.32.10/1:4/2:192.168.32.11/1:0** where:
   - 2 is the outgoing port from the workstation.
   - 192.168.32.10 is the Ethernet bridge IP address
   - 1 is the port number of chassis 1
   - 4 is the slot number of chassis 1
   - 2 is the outgoing port
   - 192.168.32.11 is the Ethernet bridge IP address
   - 1 is the port number of chassis 2
   - 0 is the slot number of chassis 2

   Figure 7. Configure Controller Connection



3. Click **Test Connection** to verify whether the controller connection is successful. The *Connection tested successfully* message is displayed when the connection is successful. Click **Save** and then click **Next** to proceed.
4. The tags available in the controller are displayed on the **State Definition** page. Select the required tags using drag and drop functionality, and add them to the **Selected tags** section. The user can also search the required tags using the search functionality and select them as required. Once the required tags are selected, click **Save** and then click **Next**.

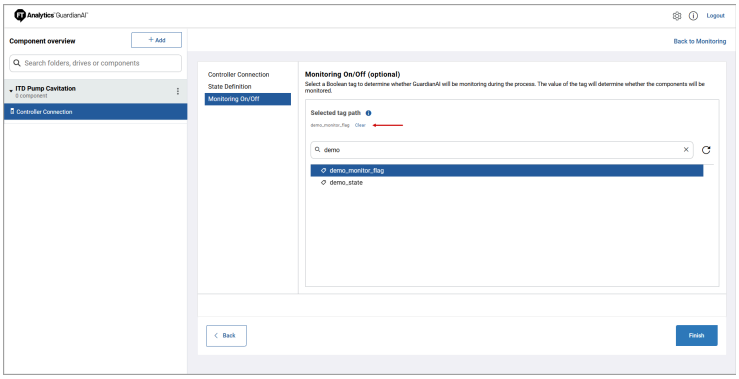
Figure 8. State Definition Tags Selection



NOTE: Tags on the **State Definition** page are sorted alphabetically. During configuration, the user cannot select the tag with nested tags. Only the lowest-level tags can be selected to define the different operational states of the component.

5. On the **Monitoring On/Off** page, select the boolean tag to determine whether GuardianAI will be monitoring during the process in the **Selected tag path** section. The boolean value of the selected tag (True/False) in the controller will determine whether the components will be monitored. Click **Finish** to complete the controller configuration.

Figure 9. Monitoring Tag Selection

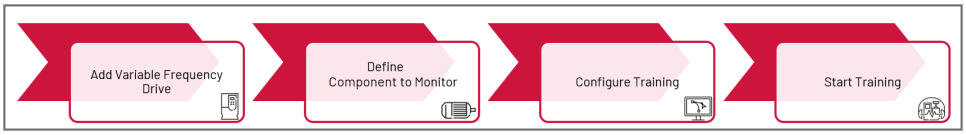


IMPORTANT: Only one boolean tag can be selected.

IMPORTANT: The user can change the controller path only after removing the tags selected in the **State Definition** and **Monitoring On/Off** pages.

Adding a new Drive and Component to Monitor

To add a new component to monitor, the user should complete the four steps summarized in the following diagram.



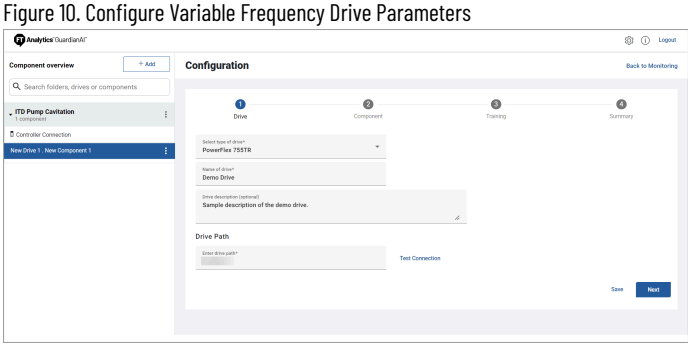
1. Add and configure the variable frequency drive. Supported drives include Powerflex 755, 755TS/TL/TM/TR/HiHP and 6000T.
2. Define the component to monitor (pump, fan, blower, motor for other component types).
3. Configure training (define the minimum and maximum frequencies).
4. Start the training process.

Configuring Drive

Perform the following steps to configure a new drive:

1. On the **Component Overview** section, click **Configuration**.
2. Select the desired folder, click **Add** > **New Drive**.
3. Provide the following details in **Drive** section of **Configuration**:
   - **Select type of drive**: Select the required type of drive. One of PowerFlex 755, 755HiHP, 755TM, 755TR, 755TL, 755TS, 6000T.
   - **Name of drive**: Provide a unique name for the drive.
   - **Drive description**: Provide a detailed description of the drive. This is optional.
   - **Drive Path**: Provide the drive path.

Figure 10. Configure Variable Frequency Drive Parameters

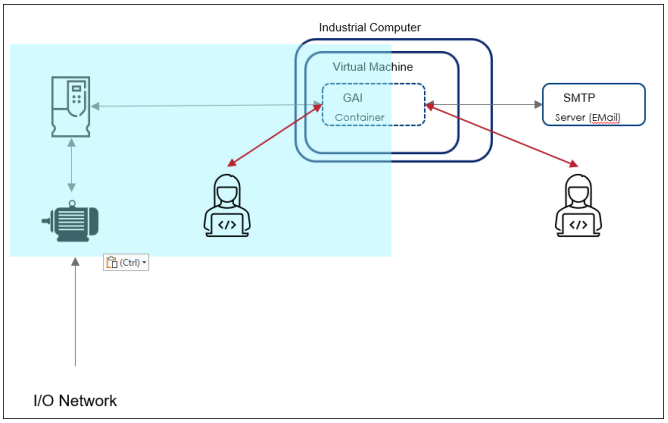


The drive path depends on the network configuration of the drive and the instance hosting GuardianAI. If both are on the same network, the drive can be accessible directly via an IP Address. In this scenario, the user can input the drive's IP address.

IP Address example format: 192.168.1.10

The following illustration depicts the instance that hosts GuardianAI and the drive on the same network location.

Figure 11. Network Illustration of Edge PC and Drive on the Same Network

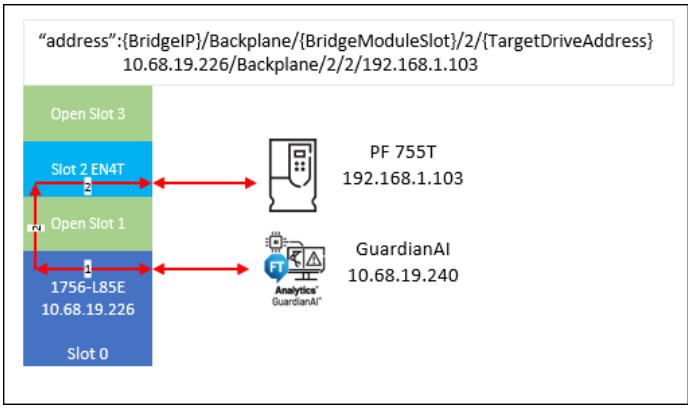


The more likely scenario is the instance that hosts the GuardianAI is not on the same network layer as the controller. In this case, the user must input the full CIP path mapping from the controller to the drive.

CIP Path format: {BridgeIP}/Backplane/{BridgeModuleSlot}/2/{TargetDriveAddress}

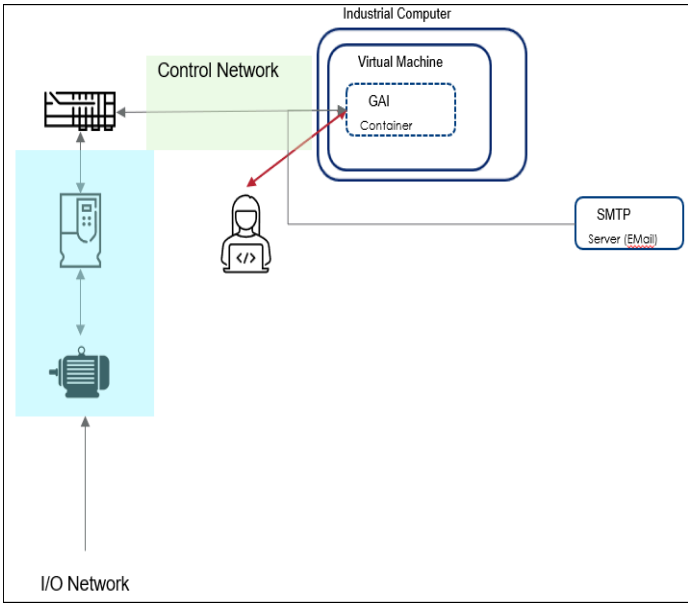
CIP Path Example: 11.70.20.214/Backplane/2/2/192.168.1.103

Figure 12. CIP Path Routing Illustration



The following illustration depicts the instance hosting GuardianAI on the control network and the variable frequency drive (VFD) on a subnet.

Figure 13. Network Illustration of Edge PC on the Control Network and Drive on a Subnet

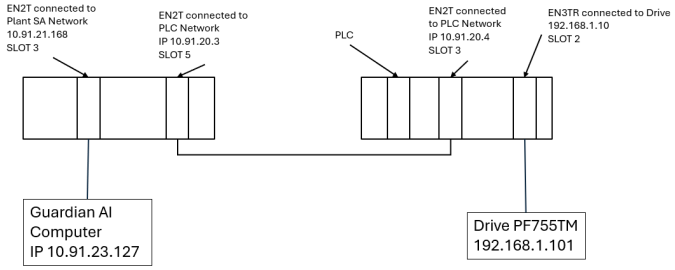


If there are multiple controller networks to connect to a drive, the user must input the full CIP path mapping from the controller to the drive as shown below:

CIP Path format for 3 networks: {BridgeIP}/Backplane/{BridgeModuleSlot}/2/{BridgeIP}/Backplane/{BridgeModuleSlot}/2/{TargetDriveAddress}

CIP Path Example: 10.91.21.168/Backplane/5/2/10.91.20.4/Backplane/2/2/192.168.1.101

Figure 14. CIP for 3 Networks



Guardian AI path: **10.91.21.168/Backplane/5/2/10.91.20.4/Backplane/2/2/192.168.1.101**

4. Click **Test Connection** to verify that the drive is connected and GuardianAI can successfully establish and validate the connection.
5. Click **Save**. The *Drive Details Updated Successfully* message displays.
6. Click **Next** to add the component details.

Configuring Component

Perform the following steps to configure a new component:

1. Provide the following details in **Component** section of **Configuration**:
   - **Name of component**: Provide a unique name for a component.
   - **Select type of component**: Select the type of component. One of Pump, Fan, Blower, Motor (used for other component types).

- **Manufacturer**: Provide the name of the manufacturer. This is optional.
- **Serial number**: Provide the serial number of the component. This is optional.
- **Model number**: Provide the model number of the component. This is optional.
- **Part number**: Provide the part number of the component. This is optional.

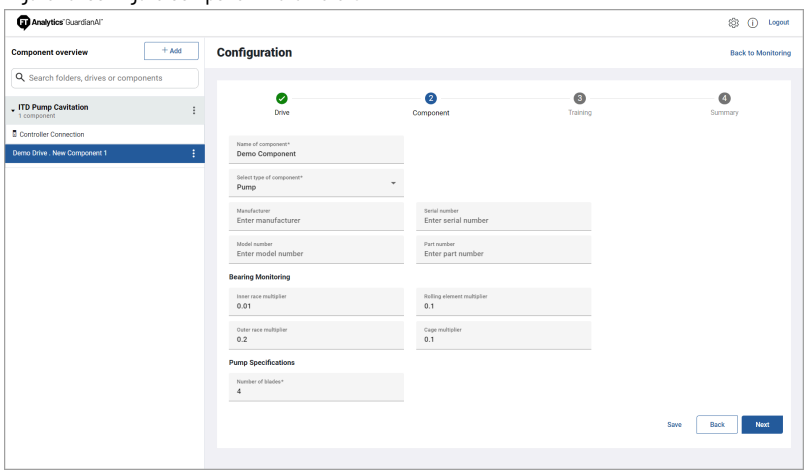
2. Provide the following details in **Bearing Monitoring** section:
   - Inner race multiplier
   - Rolling element multiplier
   - Outer race multiplier
   - Cage multiplier

   For more details on these parameters, refer to Bearing Monitoring on page 18.
3. Provide the following details in the **Pump/Fan/Blower Specifications**:

NOTE: This option is visible only when you select the Pump, Fan, or Blower as the component type.

- **Number of blades**: Provide the number of blades. The number of blades should be greater than or equal to 2 and less than or equal to 40.

Figure 15. Configure Component Parameters



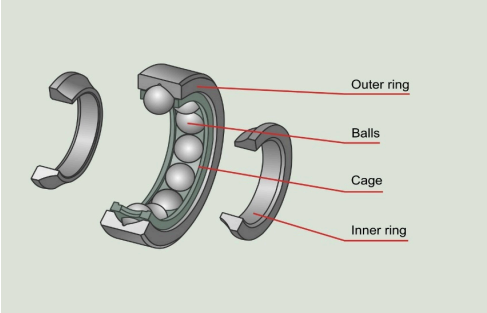
Bearing Monitoring

The bearing dimensions are used by the GuardianAI algorithm to provide first principle failure mode recommendations. The failure modes included in the bearing dimensions are ball bearing fault, inner race bearing fault, outer race bearing fault, and bearing cage fault. If the values are left empty, GuardianAI will not include those fault modes in the first principle recommendations when a deviation from normal is detected.

- **Inner Race Multiplier:** [decimal number input] - BPFI (Ball Pass Frequency Inner) or inner race failing frequency. Corresponds physically to the number of balls or rollers that pass through a given point of the inner track each time the shaft makes a complete turn.
- **Outer Race Multiplier:** [decimal number input] - BPFO (Ball Pass Frequency Outer) or outer race failing frequency. Corresponds physically to the number of balls or rollers that pass through a given point of the outer race each time the shaft makes a complete turn.

- **Rolling Element Multiplier**: [decimal number input] - BSF (Ball Spin Frequency) or rolling element failing frequency. Corresponds physically to the number of turns that a bearing ball or roller makes each time the shaft makes a complete turn.
- **Cage Multiplier**: [decimal number input] - FTF (Fundamental Train Frequency) or Cage failing frequency. Corresponds physically to the number of turns that make the bearing cage each time the shaft makes a complete turn.

Figure 16. Bearing Overview



NOTE: Rockwell Automation will be making an Excel database file available on Seismic of over 7000 bearings from common bearing manufacturers and models.

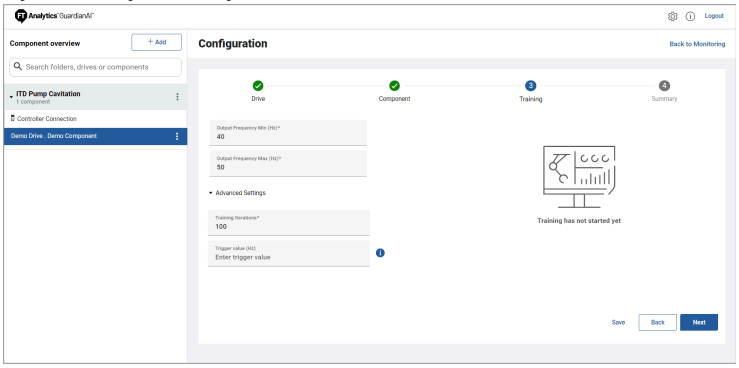
Configuring Component Training

Perform the following steps to configure component training:

1. Provide the following details in **Training** section of **Configuration**:
   - **Output Frequency Min (Hz)**: Minimum VFD command frequency of the application
   - **Output Frequency Max (Hz)**: Maximum VFD command frequency of the application
2. Provide the following details in **Advanced Settings** section:
   - **Training Iterations (Default 100)**: The number of data trends received from the variable frequency drives from GuardianAI. A lower value trains faster but generally results in a lower-quality baseline. The recommended value to use is 100 iterations. The expected time to train the baseline will be 11-18 minutes for each half-hertz increment of the operation frequency.
   - **Trigger Value Hz (Default Empty)**: An advanced trigger configured for the drive high-speed trend object. The value set will configure the drive to only send data to GuardianAI for training/monitoring when the drive operates at or above the frequency value set for the trigger. This parameter is used for advanced motion-based applications with the variable frequency drive. It will typically not be required when operating GuardianAI on pumps, fans, and blowers.

NOTE: The training performance may be impacted when running GuardianAI on Windows via a Linux virtual machine. It is also recommended to place GuardianAI as close as possible to the drive application to minimize the number of network hops.

Figure 17. Configure Training Parameters

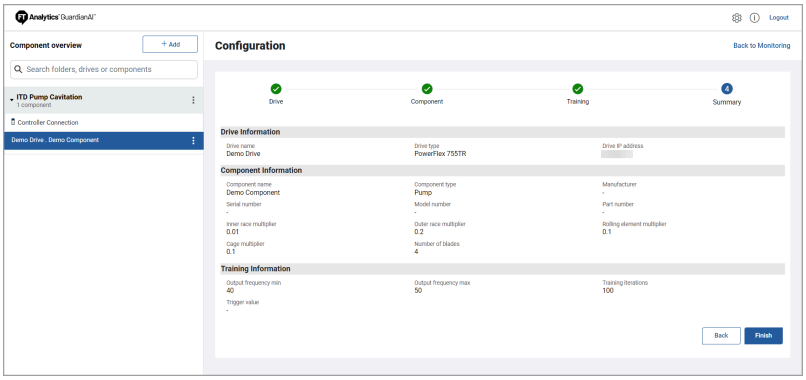


Configuration Summary

After completing the drive, component, and training steps, GuardianAI provides a summary page with final content validation. If any required field is missing, the configuration step is displayed with a yellow exclamation mark. Once all fields are completed and validated, click **Finish** to complete the new component configuration.

Once users finish the configuration, they are redirected to start training a baseline.

Figure 18. Configuration Summary and Validation



Training the Component Baseline

To start training in GuardianAI, the component should be running in normal operation. The GuardianAI is designed to observe the component under normal usage and will train models across the various speeds of the operation.

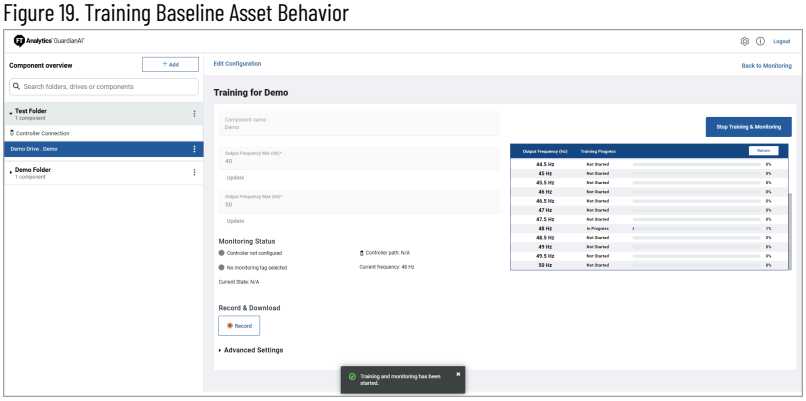
Start Training and Monitoring

Click **Start Training and Monitoring** on the Training Page. The user will see the progress bar begin to populate as data is acquired from the variable frequency drive.

The application will create a new model at each half-hertz increment of the operation speed of the component. The model is automatically switched by reading the command frequency of the drive. Once the number of training iterations is acquired, the given frequency bucket will automatically switch from training to monitoring. Multiple frequencies can be trained in parallel depending on the variability in speed of the application. GuardianAI is designed to switch automatically across frequencies between training and monitoring.

While the component is training, the user cannot edit its configuration. To make any edits, the user must click the **Stop Training and Monitoring** button.

Figure 19. Training Baseline Asset Behavior

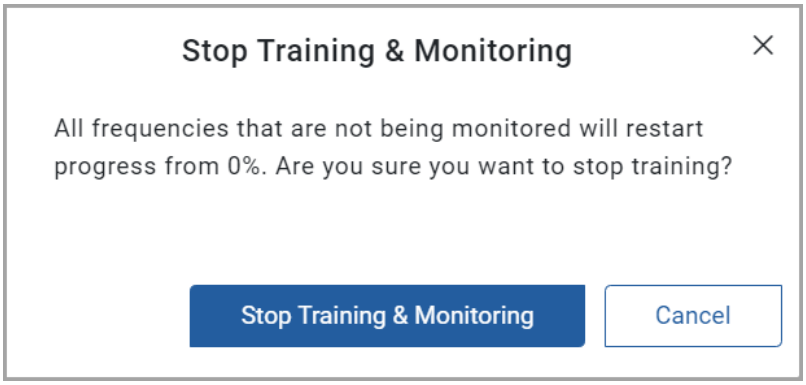


Stop Training and Monitoring

Stop Training and Monitoring will stop training and monitoring the asset. Once the user stops training, any frequency bucket in progress will be reset back to 0%. Frequencies that were already fully trained are preserved and will resume monitoring once the user starts training again.

A dialogue box will prompt the user to accept the reset of the in-progress buckets and confirm the action.

Figure 20. Stop Training Dialog Box



The user must stop training to make any edits to the component configuration.

Re-train Component

Re-training a component is essential if a major physical change is made to the system. An example might be replacing the motor or full re-alignment of a coupling. GuardianAI starts the training process under normal conditions, but it is possible there was already an existing degradation at the time when the baseline was acquired. In this scenario, the application will monitor further degradation from baseline. If a user makes a major physical change without re-training, there is a possibility that GuardianAI will view the normal operation as anomalous behavior. If too many false positives are detected after a major maintenance event, then GuardianAI should be re-trained to acquire a new baseline of the component's behavior.

Record

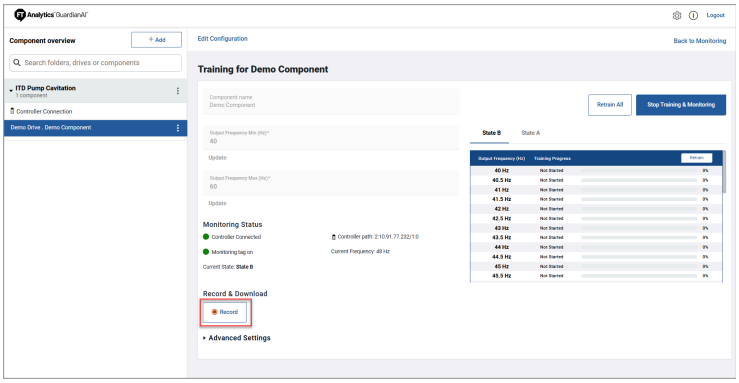
The GuardianAI allows the user to record the raw data for a specified duration and download it to analyze the data of the particular state of the component. Users can record the data for a maximum of 60 minutes.

Follow the below steps to record and download the training data:

1. On the training page, click **Record**.

NOTE: The record option is available when the component is in a training or monitoring state.

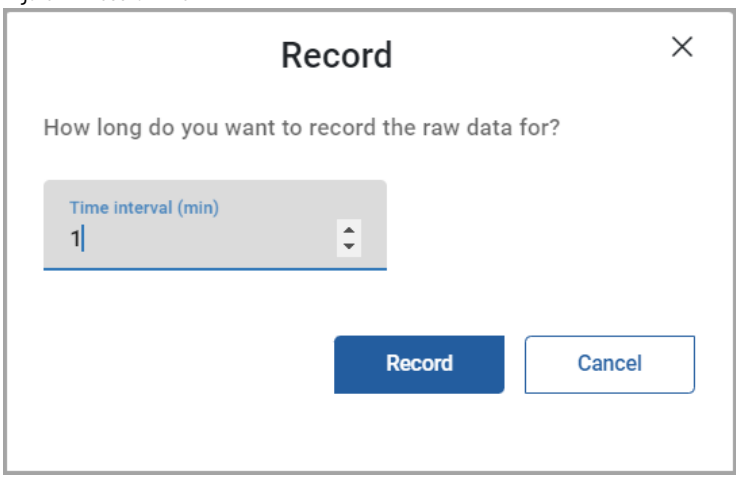
Figure 21. Record



The record pop-up window is displayed.

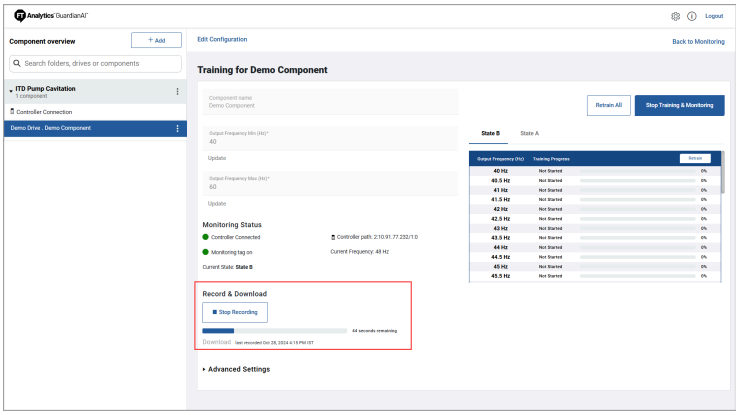
2. Provide the duration you want to record. The minimum allowed value is 1 minute, and the maximum allowed value is 60 minutes. click **Record**.

Figure 22. Record Time



The record progress bar with a countdown timer is displayed.

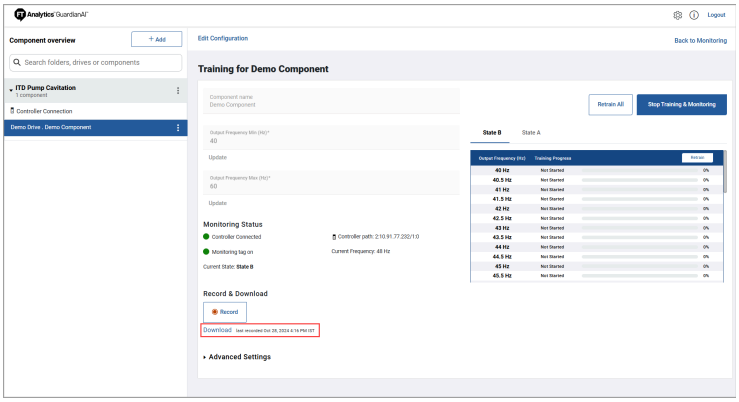
Figure 23. Record in Progress



3. After the recording is completed, click **Download** to download the training data.

NOTE: The download option is available only after the recording is completed or when the recording is stopped before completion.

Figure 24. Download



A zip file will be downloaded. Following is the naming convention for the downloaded zip file.

<Drive Name>_RecordedData_<Time stamp>.zip

- Drive Name: Name of the drive given during configuration.

Extract the zip file to view the training data in CSV format named **RecordedData.csv**.

4. While recording is in progress, the user can click **Stop Recording** to stop the process. Partially recorded data can be downloaded using the **Download** option.
5. If any existing recording is available when a user clicks on **Record**, it will be replaced with the newer one.

State Management Overview

When the GuardianAI is connected to the Controller, the user can monitor multiple baselines of a component. When the user clicks on **Start Training and Monitoring**, based on the tags selected on the **State Definition** page, GuardianAI will create a separate state with the change in the selected tag value. A separate baseline is acquired for each state, and the component will be monitored for any deviation at that particular state.

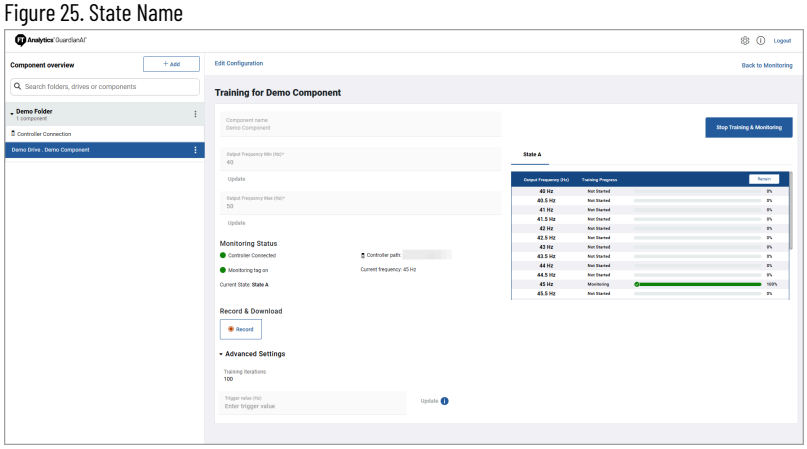
A state will be created only if the tag is valid. The tag is considered invalid if its value is empty or white space. If multiple tags are selected, at least one tag must be valid to create a state.

When the controller is not configured, the component's state is generally called the Default state. No tabs will be available.

State Name

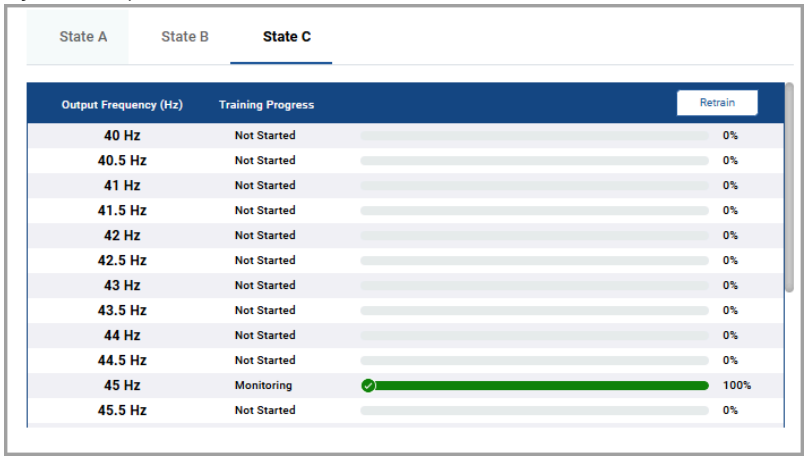
The tag value is shown as State name on the training page. If there is a change in the tag value coming from PLC, a separate tab is created for each state, using the tag value as the State name. For example, the tag selected during controller configuration is 'State A'. Hence, the state name is 'State A'.

Figure 25. State Name



Following is an example image where the component has multiple states.

Figure 26. Multiple States



In the above example, 'State C' is called the **Current State**. The name of the Current State is denoted with bold text and a blue border below it.

If multiple state definition tags are selected on the **State Definition** page during controller configuration, the state name will be displayed as "<tag1-value><tag2-value>".

Monitoring Status

On the Training page of a component, the user can view the following status in the Monitoring Status section:

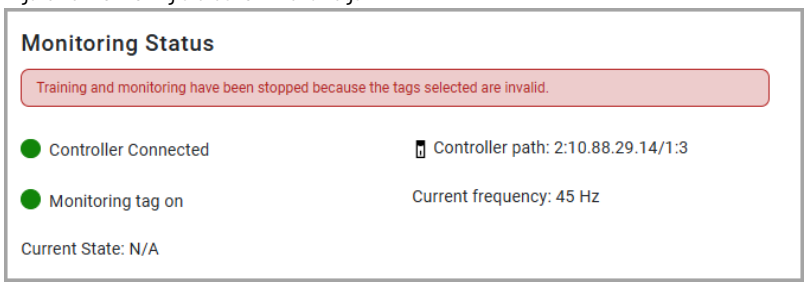
- Controller Connection Status: When the Controller is configured, the status is displayed as green and **Controller Connected**. For the default state, it is displayed as **Controller not configured**.
- Controller path: The path of the controller is displayed. For the default state, it is displayed as **N/A**.
- Monitoring Tag status: When the monitoring tag is selected, the status is displayed as green and **Monitoring tag on**. For the default state, it is displayed as grey, and **No monitoring tag selected**.
- Current Frequency: The current frequency at which the component operates is displayed.
- Current State: Name of the active state is displayed here. For the default state, it is displayed as **N/A**.

Figure 27. Monitoring Status

If only one tag is selected on the State Definition page, and if the tag is invalid, training and monitoring will be stopped. A message is displayed in red, as shown in the following image, and the current state will be shown as N/A.

If multiple tags are selected and all the tags are invalid, training and monitoring will be stopped.

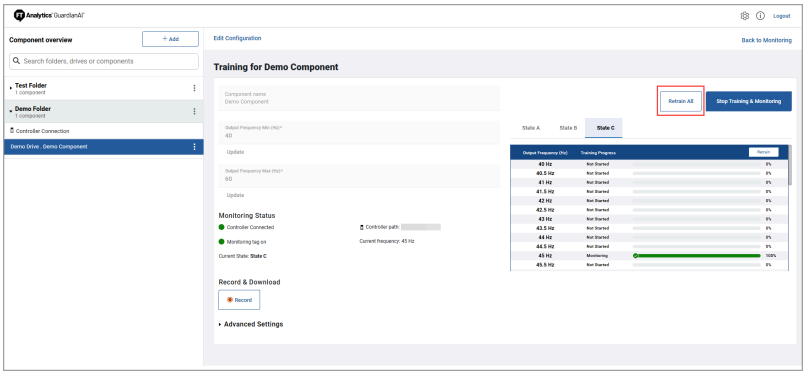
Figure 28. Monitoring Status for Invalid Tags



Retrain All

The Retrain All option helps the user to retrain all the available states of the component when a major physical change is made. The user can retrain all the states by clicking **Retrain All**. All the trained states will reset, and a new baseline will be created when the state is active.

Figure 29. Retrain All



This page has been intentionally left blank

Detecting Deviations and Failure Risks Workflow

This section provides information on detecting deviations, labelling deviations, and detecting and resolving failure risks.

Deviation to Failure Risk Workflow

This workflow is for new incoming deviations that have never been labeled within GuardianAI. The GuardianAI application is designed to learn new failure modes. Once a user has confirmed and labeled a deviation, each new occurrence of the same failure mode will surface as a failure risk.

Figure 30. Deviation to Failure Risk Workflow

As a new deviation is detected, GuardianAI will have the following workflow:

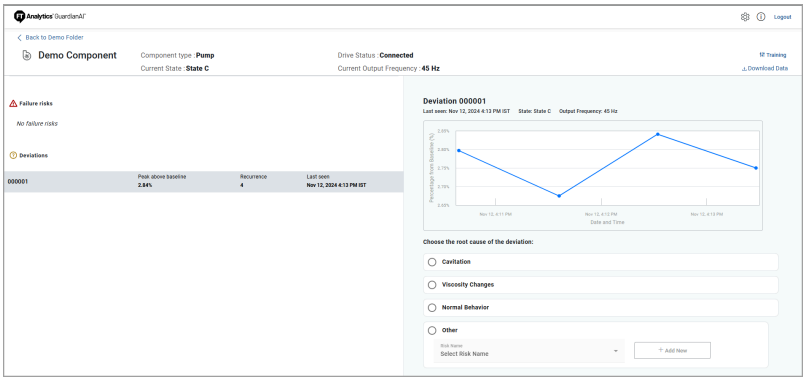
1. A deviation is detected with associated first principle recommendations.
2. The user selects between the first principle, normal operation, or creates a new label.
3. Once the detected deviation is labeled, the deviation will move to a failure risk.
4. The user should select and resolve a failure risk once the issue is fixed on the physical system. If the issue is marked as resolved but it persists, GuardianAI will re-surface the anomaly as a failure risk.

Labeling Deviations

All new anomalies detected by GuardianAI will appear as a deviation. Once a user labels a deviation, it becomes a failure risk until the user marks the anomaly as resolved. The deviation will have associated first principle recommendations. There are several ways to label the deviation:

- **First Principle**: A user can select from the first principle recommendation, the following image illustrates Cavitation and Viscosity Change.
- **Normal Behavior**: There might be a case where GuardianAI may incorrectly detect the deviation. A user can select normal behavior to train GuardianAI to recognize the detected pattern as normal.
- **Other**: A drop-down will display other labels stored in the GuardianAI database from which to select. The user can also choose to create a new label for the deviation.

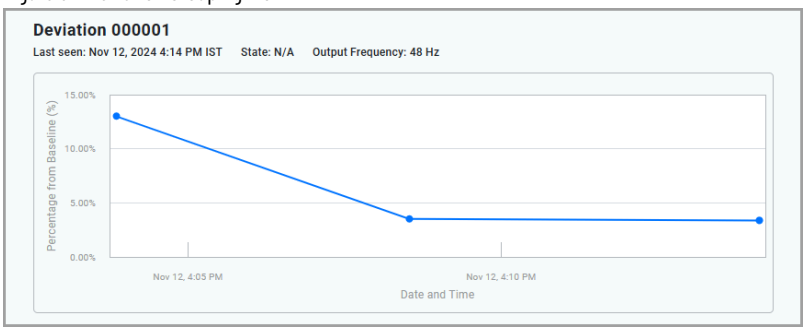
Figure 31. Deviation Detection and Grouping



Deviation Grouping

The GuardianAI application uses high-resolution three-phase current data as an input and builds a unique fingerprint (cluster) to the deviation. Deviations belonging within the same cluster will be shown as a group with a plot displaying each detected event. One point in the plot represents a deviation event. The user can use the plot to hover over a given point to examine additional details regarding the time of occurrence.

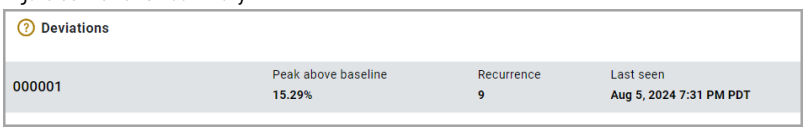
Figure 32. Deviation Grouping Plot



Suppose a pump starts cavitating at 1 am on a Saturday, and the user doesn't come in to view the anomaly until Monday. In that case, the plot will gather additional points to illustrate the continuation of the cavitation event. This grouping mechanism makes it much easier to discern different types of deviations from one another.

The deviation line item will display a high-level summary of the grouping, including a unique identifier, maximum peak above baseline, the number of recurrences, and the last timestamp at which this deviation pattern was detected.

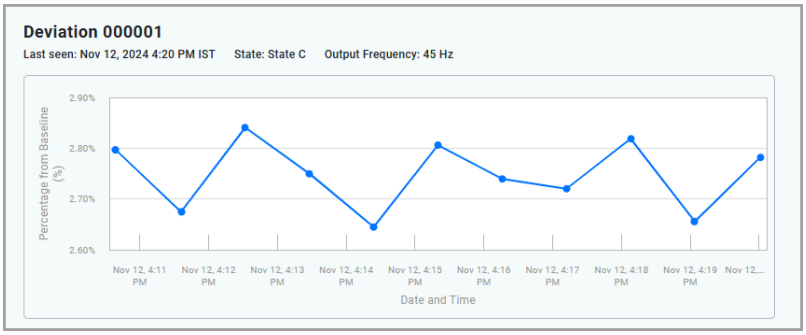
Figure 33. Deviation Summary



If there are multiple states, a separate deviation line item is displayed for each state. In other words, all the deviation associated to all the states will be displayed under **Deviations** section.

When the user selects a particular deviation item, the associated deviation grouping plot is displayed.

Figure 34.



First Principle Failure Mode Recommendations

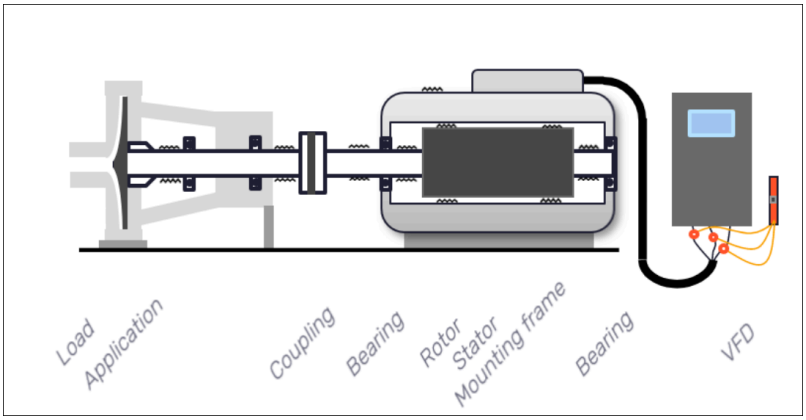
When providing first principle recommendations, some frequencies may overlap resulting in several suggestions made by GuardianAI.

For motor analytics, GuardianAI can differentiate the variation between bearing faults, mounting/coupling, and load application. In the example of a bearing fault, the user will see multiple recommendations including Ball, Inner Race, Outer Race, and Cage. The following image illustrates the overlapping recommendations for motor, pump, and fan/blower first principle recommendations

Figure 35. First Principle Recommendations for Motor, Pump, Fan, and Blower

Pumps, fans, and blowers are specific applications of motor analytics. When a user configures a pump, fan, or blower, GuardianAI will provide first principle recommendations for the specific application and the motor analytics. As illustrated below, the analysis from GuardianAI is inclusive of the motor, coupling, and Load application.

Figure 36. Analysis of a Full System (Motor, Coupling, and Load Application)



For additional details regarding first principle failure modes, refer to Appendix A: First Principle Failure Modes.

Normal Operation

In the event GuardianAI incorrectly identifies a deviation, a user can label it as normal behavior to help reinforce normal vs anomalous behavior. If a user selects a normal when there is an anomalous behavior, retraining of the component may be required.

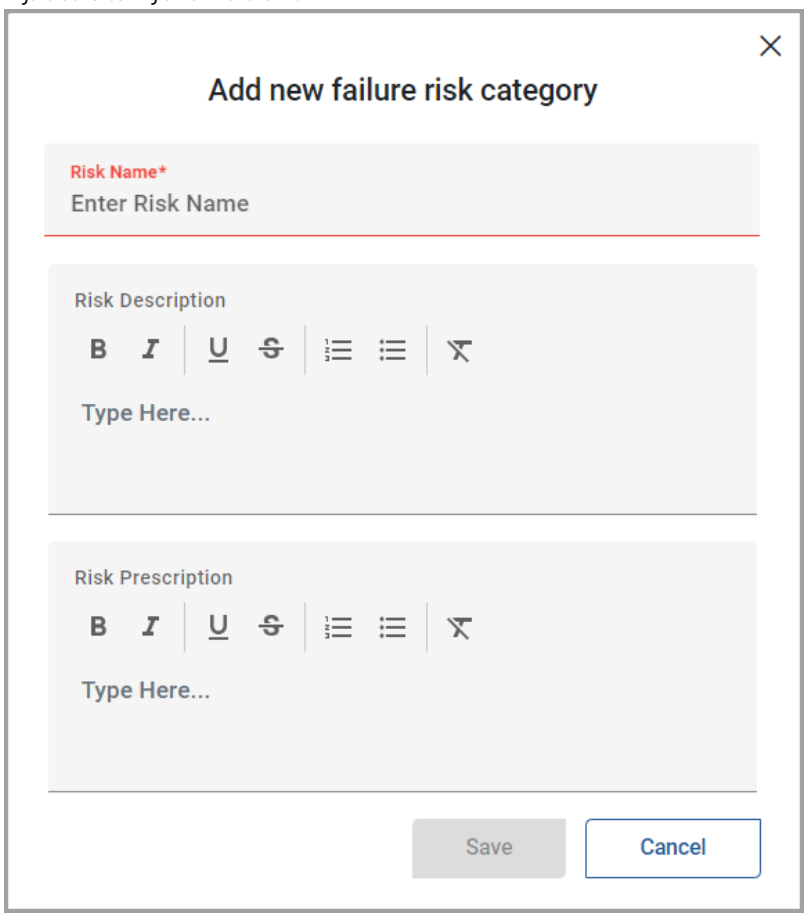
Creating a New Deviation Label

If none of the first principle recommendations apply, a user can choose to create a new label. To do so, a user should select the "Other" radio button and click on Add New.

Figure 37. Other & Add New Deviation Label

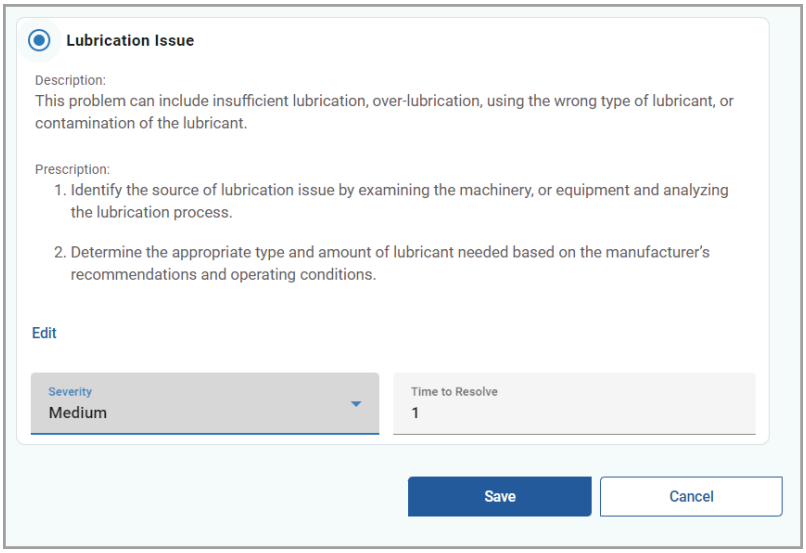
A dialogue box is displayed with the fields to create the new failure Risk label. The label includes the name, descriptions, and prescription (optional).

Figure 38. Creating a New Failure Risk



Upon creating the new label, the user can associate severity and recommended time to resolve the deviation (in days). The time to resolve must be in between 1 and 365.

Figure 39. Severity and Time to Resolve



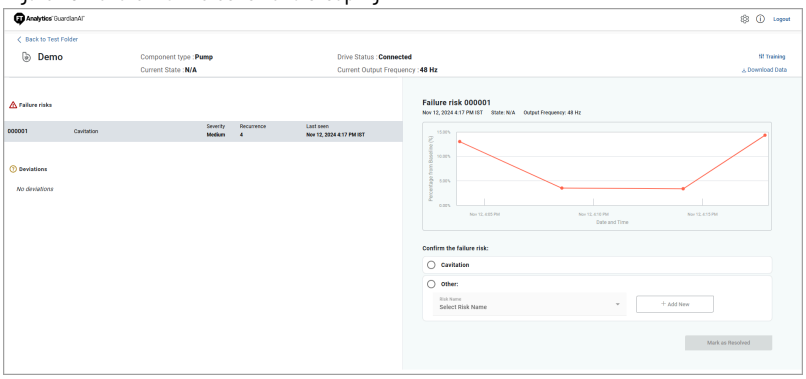
Detecting Failure Risks

Failure risks are deviations that have been labeled and confirmed by a user. If an anomaly is detected again, GuardianAI will automatically display it as a failure risk with the associated label a user provided when they first encountered the anomaly in the deviation workflow.

A user can choose to change the label if their root cause analysis yields a different outcome, by using the Other label workflow. The steps are identical to labeling a new deviation.

The purpose of the failure risk workflow is to reduce the time spent having to run through maintenance investigation and root cause analysis. After resolving the anomaly in the physical system being monitored, a user can mark the failure risk as resolved to remove it from the user interface. GuardianAI will bring back the failure risk if the signature is detected again.

Figure 40. Failure Risk Detection and Grouping

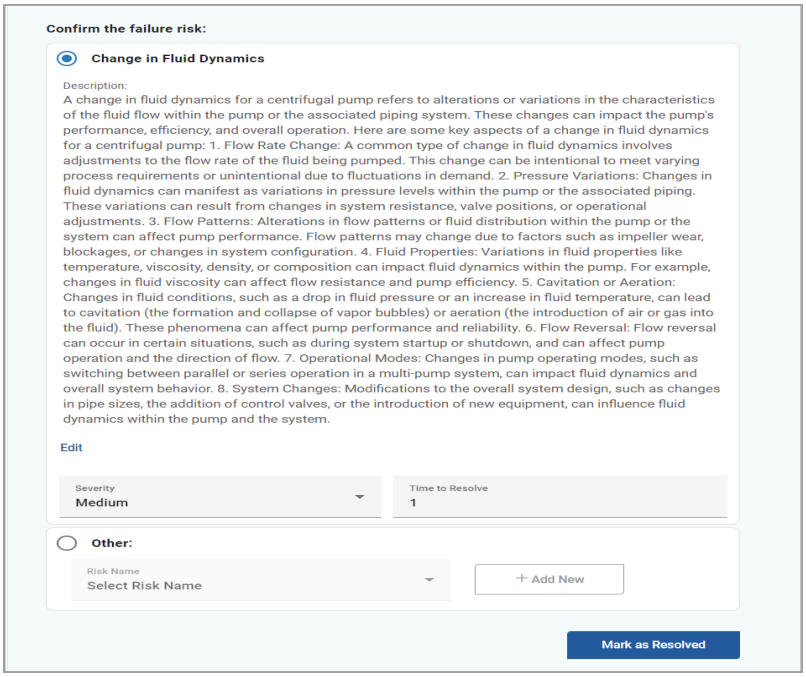


All failure risks of all the states associated to the component will be displayed as separate item in **Failure risks** section. When the user selects a particular failure risk item, associated plot will be displayed.

Resolving Failure Risks

To resolve a failure risk, confirm the corresponding label and select **Mark as resolved**.

Figure 41. Resolve a Failure Risk

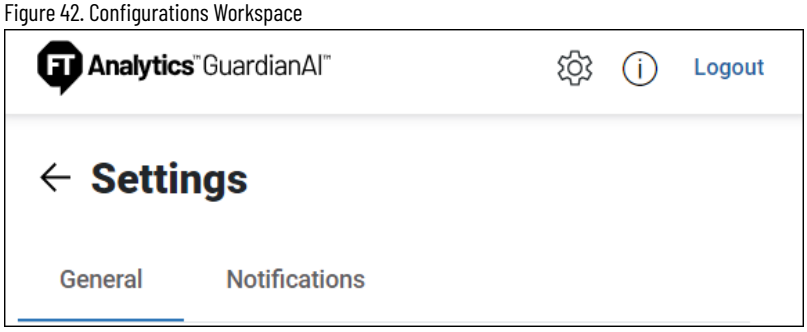


A user can also change the failure risk label and create a new one using the steps illustrated in the deviation workflow section on Creating a New Deviation Label. The user can select the **Other** option and either choose a label from the drop-down or create a new failure risk label.

Configuration Workspace

In the upper-right corner of the screen, GuardianAI provides a gear icon allowing a user to configure application parameters along with email notifications.

Figure 42. Configurations Workspace



Notifications

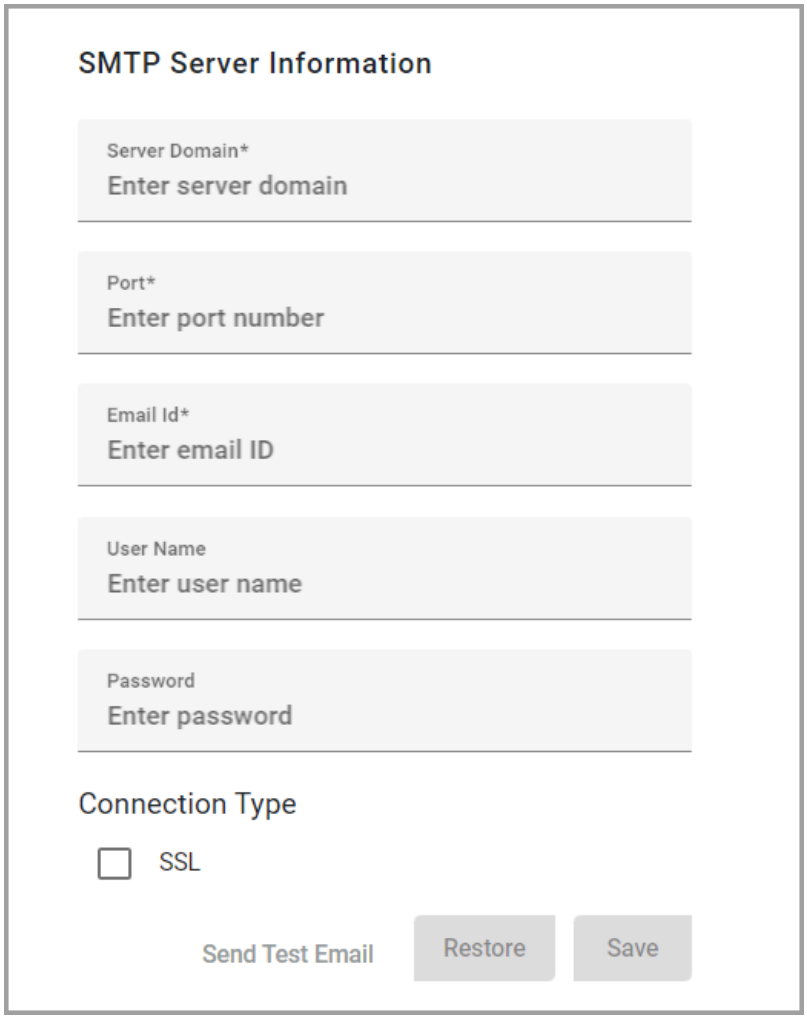
GuardianAI provides a combination of event-based notifications and summary reports configured on a daily, weekly, or monthly basis. Configuring notifications requires a connection to the SMTP server, turning on notifications, and creating a distribution list. All users on the distribution list will receive notifications.

Configure SMTP Server

To configure the SMTP Server, a user should first go to the Notifications settings by selecting the gear icon in the upper right of the application. The instance hosting GuardianAI should have visibility to the network hosting the SMTP server. To establish the connection, the following parameters will need to be configured. It may be required to consult with an IT department to obtain an SMTP server:

1. **Server Domain**: The domain address of the SMTP server (consult with IT)
2. **Port Number**: SMTP server port, common ports may be 25, 465, or 587 (consult with IT)
3. **Email Id**: The email ID displayed to the email recipient (example: noreply.guardianAI@rockwellautomation.com)
4. **Username**: Username to authenticate with the SMTP server (consult with IT)
5. **Password**: password to authenticate with the SMTP server (consult with IT)
6. **SSL Connection (optional)**: Enable SSL encryption when communicating between FactoryTalk Analytics GuardianAI and the SMTP server

Figure 43. SMTP Server Configuration

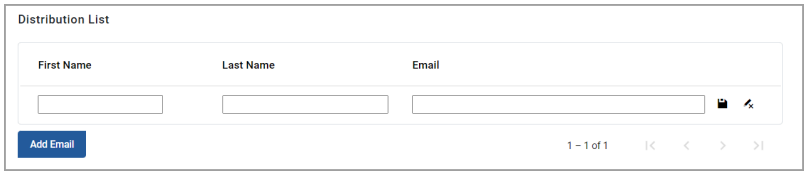


Adding Users and Recipients

To manage the distribution list, add users by going to the add email button on the notification settings page. Input the First Name, Last Name, and Email, and click the save icon to the right of the email input field.

Click the **Add Email** button to add additional users to the list.

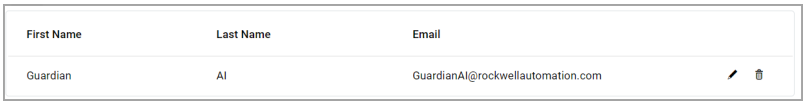
Figure 44. Manage User Distribution List



Editing a User in the Distribution List

To edit a user in the distribution list, select the pencil icon in line with the desired user to edit. Make the necessary changes to the First Name, Last Name, and Email, and select the save icon.

Figure 45. Edit a User in the Distribution List



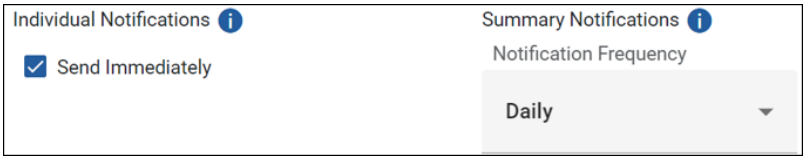
Removing a User from the Distribution List

To remove a user from the distribution list, select the delete icon in line with the desired user to remove. FactoryTalk Analytics GuardianAI will provide a pop-up asking to confirm the step to delete the user.

Notifying Users and Recipients

FactoryTalk Analytics GuardianAI sends two types of notification emails.

Figure 46. Email Notification Frequency Configuration



- **Individual event notifications**: These notifications are sent when a deviation or failure risk is detected on an asset.
- **Summary notifications**: These notifications are sent on a configured cadence regarding all active deviations and failure risks across all assets monitored by FactoryTalk Analytics GuardianAI.

To enable individual event notifications, select the checkbox labeled **Send Immediately**. FactoryTalk Analytics GuardianAI sends email notifications for every deviation and failure risk event detected on all assets under active monitoring.

To enable summary email notifications, select the dropdown under Notification Frequency to configure the cadence by which to send the summary emails, options include:

- **Disabled**: Email summaries are disabled and will not be sent on any cadence.
- **Daily**: Sent at 8 AM every day based on the time zone configured for the local installation of FactoryTalk Analytics GuardianAI.
- **Weekly**: Sent at 8 AM every Monday based on the time zone configured for the local installation of FactoryTalk Analytics GuardianAI.
- **Monthly**: Sent at 8 AM on the first Monday of every month based on the time zone configured for the local installation of FactoryTalk Analytics GuardianAI.

Notification Frequency

This topic provides information about the email notification frequency.

- **Individual Notifications (if enabled)**
  - **Deviations**
    - Each deviation will provide an email when generated.
    - Subsequent grouped notifications will never generate an email.

- **Failure Risks**
  - Moving a deviation to failure risk will not generate an immediate notification.
  - Each failure risk will notify up to exactly 1 time per day if generated again.
  - A failure risk will never notify on the same day it is converted to from a deviation.
  - This means if the following occurs: Failure Risk Generated (email generated) -> Resolved -> Failure risk generates again (Same calendar day) the second generated risk would not trigger an email.

- **Summary Notifications (all times local)**
  - **Daily**: 8 AM each day
  - **Weekly**: 8 AM Monday
  - **Monthly**: 8 AM first Monday
  - If the application is restarted, the time to notify will always be the next notification point, starting from the next calendar day.
    - Example: If the application is set to 'Daily', and the application restarts at 3 PM, it would generate at 8 AM the next day
    - Example: If the application is set to 'Daily' and the application restarts at 7:55 AM, it would generate at 8 AM the next day (skipping the 8 AM 5 minutes from restart)

Email Template

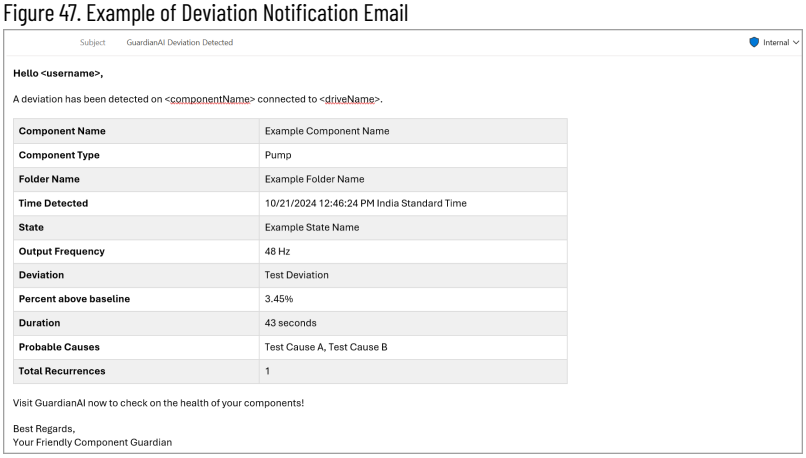
This topic describes the email templates for single event notification and summary notification.

Single Event Notification

The single event notification is intended to send an immediate notification on any deviation or failure risk regarding an component monitored by GuardianAI.

For a **deviation**, the notification contains the information shown in the following image.

Figure 47. Example of Deviation Notification Email


Subject GuardianAI Deviation Detected

Internal

Hello <username>,

A deviation has been detected on <componentName> connected to <driveName>.

Component Name	Example Component Name
Component Type	Pump
Folder Name	Example Folder Name
Time Detected	10/21/2024 12:46:24 PM India Standard Time
State	Example State Name
Output Frequency	48 Hz
Deviation	Test Deviation
Percent above baseline	3.45%
Duration	43 seconds
Probable Causes	Test Cause A, Test Cause B
Total Recurrences	1

Visit GuardianAI now to check on the health of your components!

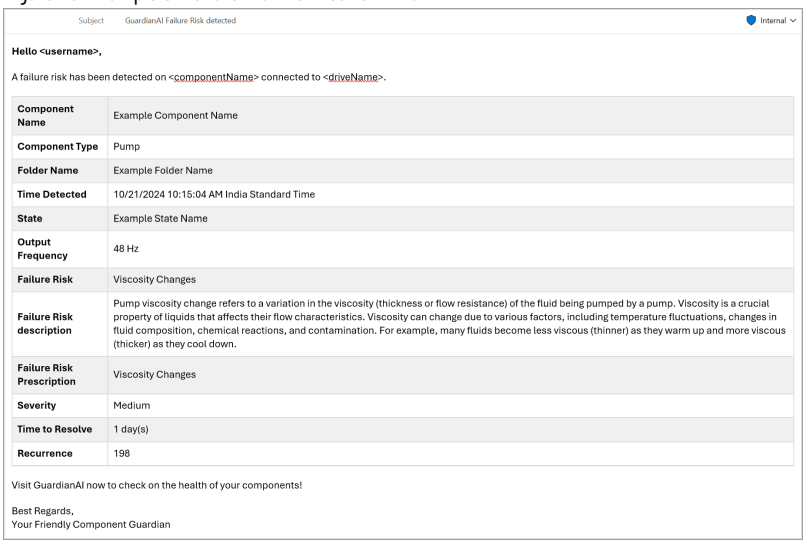
Best Regards,
Your Friendly Component Guardian

- **Component Name**: Name of the component given during the first-time configuration.
- **Component Type**: Pump, Fan, Blower, or Motor Analytics.
- **Folder Name**: The folder name containing the drive and component combination.
- **Time Detected**: The time at which the event was detected based on the local time zone of the GuardianAI instance.

- **State**: The state at which the component is operating.
- **Output Frequency**: The output frequency of the drive.
- **Deviation**: Name of the deviation
- **Percent above baseline**: The percentage deviation from baseline.
- **Duration**: Amount of time the deviation has persisted.
- **Probable Causes**: First Principle Failure mode recommendations.
- **Number of recurrences**: The amount of time the deviation has been detected.

For a **failure risk**, the notification contains the information shown in the following image.

Figure 48. Example of Failure Risk Notification Email



Subject GuardianAI Failure Risk detected

Internal

Hello <username>,

A failure risk has been detected on <componentName> connected to <driveName>.

Component Name	Example Component Name
Component Type	Pump
Folder Name	Example Folder Name
Time Detected	10/21/2024 10:15:04 AM India Standard Time
State	Example State Name
Output Frequency	48 Hz
Failure Risk	Viscosity Changes
Failure Risk description	Pump viscosity change refers to a variation in the viscosity (thickness or flow resistance) of the fluid being pumped by a pump. Viscosity is a crucial property of liquids that affects their flow characteristics. Viscosity can change due to various factors, including temperature fluctuations, changes in fluid composition, chemical reactions, and contamination. For example, many fluids become less viscous (thinner) as they warm up and more viscous (thicker) as they cool down.
Failure Risk Prescription	Viscosity Changes
Severity	Medium
Time to Resolve	1 day(s)
Recurrence	198

Visit GuardianAI now to check on the health of your components!

Best Regards,
Your Friendly Component Guardian

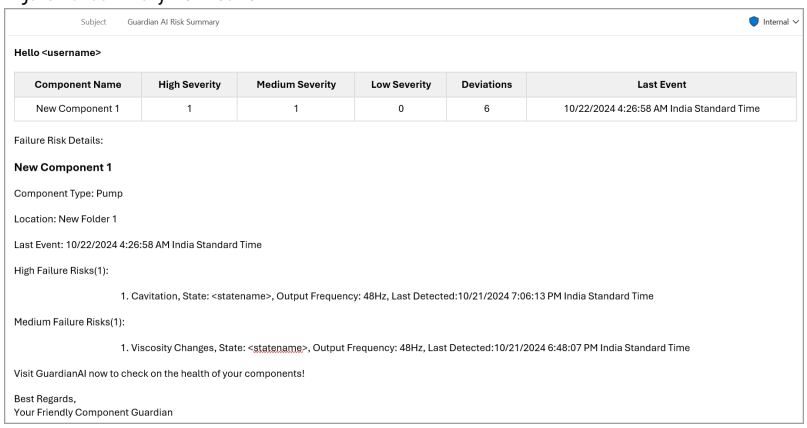
- **Component Name**: Name of the component given during the first-time configuration.
- **Component Type**: Pump, Fan, Blower, or Motor Analytics.
- **Folder Name**: The folder name containing the drive and component combination.
- **Time Detected**: The time at which the event was detected based on the local time zone of the FactoryTalk Analytics GuardianAI instance.
- **State**: The state at which the component is operating.
- **Output Frequency**: The output frequency of the drive.
- **Failure Risk Name**: The name of the failure risk, this is given during the labeling process for a deviation.
- **Failure Risk Description**: The description of the failure risk indicates additional details about the detected anomaly.
- **Failure Risk Prescription (if exists)**: Recommendation regarding the action to take to resolve the failure risk.
- **Severity**: A ranking of the severity (low, medium, high).
- **Time to Resolve**: Time expected to resolve the failure risk.
- **Recurrence**: The number of times the failure risk has been detected.

Summary Notification

The summary notification provides a high-level table regarding all unlabeled deviations and unresolved failure risks for all assets monitored by GuardianAI. The table rows will show the asset names, with one row dedicated to each

component. The table columns include the count of unresolved Failure Risks ranked by severity, along with the count of unlabeled existing deviations with the last column showing the time stamp of the last detected event. Below the table is the enumeration of each asset with additional details regarding the detected failure risks and deviations.

Figure 49. Summary Notification



General Settings

This section provides information about about general settings such as setting time zone, updating password, and configuring SSL certificate.

Setting Time Zone

The Time zone is used by FactoryTalk Analytics GuardianAI to set all time stamps for deviations and failure risks in the user experience. Email notifications also reference timestamps to notify the occurrence of those deviations. It is recommended to set the time zone to reflect the location where the FactoryTalk Analytics GuardianAI edge node is installed to reflect the local time at which the anomalies are detected.

Figure 50. General Settings - Time zone Configuration

Changing Login Password

To change the password to the login screen, a user can go to settings and utilize the change password option. Input the current password, and the new password, confirm the new password, and click on the update button.

Figure 51. General Settings - Change Password

Configuring SSL Certificate

By default, FactoryTalk Analytics GuardianAI is configured with a self-signed certificate. A secure sockets layer (SSL) certificate refers to a file hosted within the webpage's origin server, which holds the data that browsers access when you are viewing and interacting with the page. The certificate may be self-signed or signed (issued) by a third party. Customers can import an issued certification and import it by utilizing the Import SSL Certificate section.

Figure 52. General Settings - Import SSL Certificate

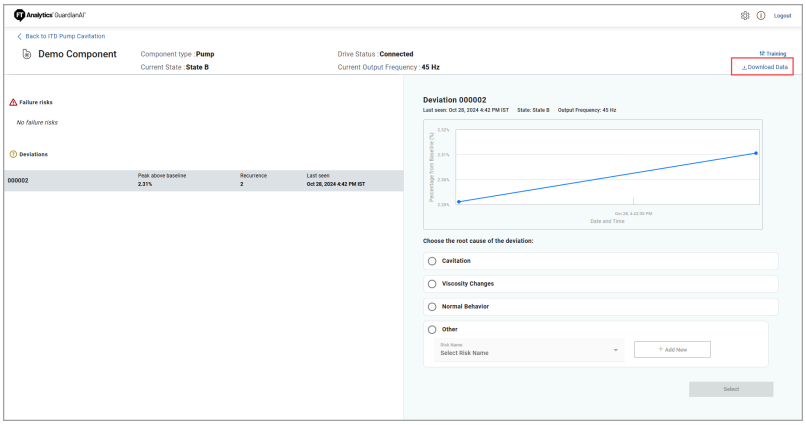
This page has been intentionally left blank

Download Raw Data

GuardianAI allows the user to download the raw data of training, deviation, and failure risk to analyze or enable bulk training on a new algorithm.

Users can download the raw data from the single component view page. Click **Download Data** to download. The user can download the data of all states of the component if multiple states are available.

Figure 53. Download Data



Following is the folder naming convention for the downloaded zip file:

<Drive Name>_RawData_<Time stamp>.zip

- Drive Name: Name of the drive given during configuration.
- Time Stamp: Time when the download occurs.

The data for each drive frequency will be stored in a separate folder. For example, data related to 48 Hz frequency will be stored in a folder named **48**. Multiple folders will be created if the component is trained with multiple frequencies.

Each frequency folder contains the following data:

- Training: The data for training is available as **Training.zip** file.
- Deviation: The data for deviation is available as **<DeviationID>.zip** inside a sub-folder named **Deviation**.
- FailureRisk: The data for FailureRisk is available as **<FailureRiskID>.zip** inside a sub-folder named **FailureRisk**.

This page has been intentionally left blank

Appendix A: First Principle Failure Modes

Appendix A provides the list first principle failure modes embedded within FactoryTalk Analytics GuardianAI for Motors, Pumps, and Fans and Blowers.

Motor Analytics

The following table contains the first principle failure modes embedded within FactoryTalk Analytics GuardianAI for motors. These may be provided as recommendations during deviation detection based on the matching frequency analysis of the deviation.

Failure Mode Label	Description
Unbalance	Unbalance may present in two ways, overhung or coupled. Consider two scenarios: • A shaft supported by bearings on either end and fitted with bladed wheels or other masses, has an imbalance at some location other than dead-center. In this case, called 'coupled' unbalance, an imbalance nearer to one bearing than the other would cause the shaft to wobble. • An overhung shaft, supported only on one end, and that has an imbalance some distance from the supporting bearing: Since the mass relative to the bearing is consistent, shaft motion is likely to be consistent. While it would move more at further distances from the bearing, it would always move in the same direction.
Shaft Misalignment	Misalignment refers to a condition where the components of a motor system, such as the motor shaft and the driven equipment (e.g., a pump or a fan), are not properly aligned with each other. There are several ways misalignment can occur between two shafts including angular, parallel and, if fitted with a rolling element bearing, the bearing could be misaligned with the shaft
Loose Structural Mounting (Soft Foot)	This can be caused by the structural looseness of machine mounting. Distortion of the base is likely to cause 'soft foot' problems
Mechanical Looseness	Mechanical looseness refers to a condition where the components of a motor system are not securely fastened or sufficiently connected
Rotor Rub	Rotor rub refers to a mechanical issue that occurs when the rotor (the rotating part of an electric motor) comes into contact with the stator (the stationary part of the motor). A rotor rub can occur in a radial direction at a seal, for example, or in the axial direction, due to uneven thermal growth between a turbine rotor and its casing. In any case, it is a rub, either through a complete shaft revolution or just during a part of a revolution, between rotating and stationary components.
Ball Bearing Fault	Common types of bearing ball faults in motors include: 1. Ball Bearing Wear: Over time, the constant movement and friction within the bearing can cause wear and tear on the ball bearings. This wear may manifest as pitting, scoring, or general surface deterioration, ultimately leading to reduced bearing performance.

Failure Mode Label	Description
	2. Ball Bearing Spalling: Spalling occurs when small pieces of the bearing material break away, leaving behind rough or uneven surfaces. This can result from excessive loads, improper lubrication, or other factors that cause localized stress on the bearing balls. 3. Bearing Ball Cracks: Cracks in bearing balls can be caused by a variety of factors, including overloading, improper installation, or manufacturing defects. Cracked balls can lead to increased friction and vibration within the bearing. 4. Ball Bearing Misalignment: Misalignment of the bearing balls can result from factors such as shaft misalignment or excessive axial or radial loads. Misalignment can lead to uneven wear and increased stress on the balls.
Inner Race Bearing Fault	The inner race of a bearing is the part of the bearing that directly contacts and supports the motor shaft. Common types of inner race bearing faults in motors include: 1. Inner Raceway Wear: Over time, the constant movement and friction within the bearing can cause wear and tear on the inner raceway. This wear may manifest as pitting, scoring, or general surface deterioration, ultimately leading to reduced bearing performance. 2. Inner Raceway Cracking: Cracks in the inner raceway can be caused by factors such as overloading, improper installation, or manufacturing defects. Cracks can lead to increased stress concentrations and reduced bearing load-carrying capacity. 3. Inner Raceway Fretting: Fretting refers to small-scale wear and corrosion that can occur at the contact interface between the inner race and the motor shaft. It often results from microscopic relative motion between the surfaces, which can lead to surface damage and pitting. 4. Indentations or Bruising: Sudden impacts or heavy shock loads can cause indentations or bruising on the inner raceway. These physical deformations can lead to uneven loading and increased stress on the bearing.
Outer Race Bearing Fault	The outer race of a bearing is the part of the bearing that is stationary and typically housed in the motor's casing or housing. Common types of outer race bearing faults in motors include: 1. Outer Raceway Wear: Over time, the constant movement and friction within the bearing can cause wear and tear on the outer raceway. This wear may manifest as pitting, scoring, or general surface deterioration, ultimately leading to reduced bearing performance. 2. Outer Raceway Cracking: Cracks in the outer raceway can occur due to factors such as overloading, improper installation, or manufacturing defects. Cracks can lead to increased stress concentrations and reduced bearing load-carrying capacity. 3. Outer Raceway Fretting: Fretting refers to small-scale wear and corrosion that can occur at the contact interface between the outer race and the

Failure Mode Label	Description
	bearing housing or casing. It often results from microscopic relative motion between the surfaces, which can lead to surface damage and pitting. 4. Indentations or Bruising: Sudden impacts or heavy shock loads can cause indentations or bruising on the outer raceway. These physical deformations can lead to uneven loading and increased stress on the bearing.
Bearing Cage Fault	A bearing cage fault, refers to an issue that occurs within the bearing cage, also known as the bearing retainer or bearing separator, of a ball or roller bearing used in an electric motor. Common types of bearing cage faults in motors include: 1. Cage Wear or Erosion: Over time, the constant movement and friction within the bearing can cause wear or erosion of the bearing cage material. This can lead to the misalignment or irregular positioning of rolling elements, affecting bearing performance. 2. Cage Cracking or Fracture: The bearing cage can develop cracks or fractures due to factors such as excessive loads, shock loads, or manufacturing defects. Cracks in the cage can disrupt the proper functioning of the bearing by allowing the rolling elements to move irregularly. 3. Cage Deformation: The bearing cage can become deformed or distorted due to high temperatures or overloading. Deformation can result in misalignment of the rolling elements, leading to increased friction and wear. 4. Cage Jamming: In cases where debris or contamination enters the bearing, it can become lodged in the bearing cage, preventing the free movement of rolling elements. This can cause significant bearing issues and reduce motor performance.

Pump First Principle Failure Modes

The following table contains the first principle failure modes embedded within FactoryTalk Analytics GuardianAI for pumps. Pumps are a specific application of motor analytics. When monitoring a pump, FactoryTalk Analytics GuardianAI will provide a combination of pump and motor failure modes. These may be provided as recommendations during deviation detection based on the matching frequency analysis of the deviation.

Failure Mode Label	Description
Impeller Unbalance	Pump impeller unbalance refers to an irregular distribution of mass or weight within the impeller of a centrifugal pump. The impeller is a critical rotating component in a centrifugal pump responsible for generating the flow of fluid. When there is an imbalance in the impeller, it means that certain parts of the impeller are heavier or unevenly distributed compared to others.
Blade Fault	A pump blade fault refers to a problem or issue that affects the blades of the impeller in a centrifugal pump. The impeller is a critical component of a centrifugal pump responsible for generating the flow of fluid by rotating and creating a centrifugal force that propels the liquid. Pump blade faults can have various

Failure Mode Label	Description
	causes and consequences, impacting the pump's performance and reliability. Here are some common types of pump blade faults: 1. Erosion: Erosion occurs when the impeller blades gradually wear away due to the abrasive nature of the fluid being pumped. This is particularly common in pumps handling fluids with suspended solids or corrosive properties. Erosion can result in reduced efficiency and flow rates. 2. Cavitation Damage: Cavitation is a phenomenon that occurs when the pressure of the fluid drops below its vapor pressure, causing the formation and collapse of vapor bubbles near the impeller blades. This can lead to pitting, erosion, or surface damage on the blade tips, reducing their effectiveness. 3. Cracks or Fractures: Blade cracks or fractures can develop due to factors such as mechanical stress, excessive loads, or manufacturing defects. Cracked or fractured blades can lead to reduced structural integrity and efficiency. 4. Bending or Distortion: Blades may become bent or distorted due to impacts, excessive forces, or unbalanced loads. This can result in uneven flow and reduced pump performance. 5. Wear and Tear: General wear and tear can occur over time, causing blade surfaces to lose their smoothness and shape. This can lead to reduced efficiency and increased energy consumption. 6. Buildup of Deposits: Some fluids may leave deposits on the impeller blades, such as scale or sludge. These deposits can disrupt the flow pattern and reduce pump performance.
Cavitation	Cavitation in centrifugal pumps is a fluid dynamic phenomenon characterized by the formation of vapor-filled cavities or bubbles within the pump due to low-pressure regions in the fluid flow. These cavities or bubbles form when the pressure of the liquid being pumped drops below its vapor pressure, causing the liquid to vaporize temporarily. When these vapor bubbles move to regions of higher pressure within the pump, they collapse or implode, creating shockwaves and intense localized pressure fluctuations.
Viscosity Changes	Pump viscosity change refers to a variation in the viscosity (thickness or flow resistance) of the fluid being pumped by a pump. Viscosity is a crucial property of liquids that affects their flow characteristics. Viscosity can change due to various factors, including temperature fluctuations, changes in fluid composition, chemical reactions, and contamination. For example, many fluids become less viscous (thinner) as they warm up and more viscous (thicker) as they cool down.
Change in Fluid Dynamics	A change in fluid dynamics for a centrifugal pump refers to alterations or variations in the characteristics of the fluid flow within the pump or the associated piping system. These changes can impact the pump's performance, efficiency, and overall operation.

Failure Mode Label	Description
	Here are some key aspects of a change in fluid dynamics for a centrifugal pump: 1. Flow Rate Change: A common type of change in fluid dynamics involves adjustments to the flow rate of the fluid being pumped. This change can be intentional to meet varying process requirements or unintentional due to fluctuations in demand. 2. Pressure Variations: Changes in fluid dynamics can manifest as variations in pressure levels within the pump or the associated piping. These variations can result from changes in system resistance, valve positions, or operational adjustments. 3. Flow Patterns: Alterations in flow patterns or fluid distribution within the pump or the system can affect pump performance. Flow patterns may change due to factors such as impeller wear, blockages, or changes in system configuration. 4. Fluid Properties: Variations in fluid properties like temperature, viscosity, density, or composition can impact fluid dynamics within the pump. For example, changes in fluid viscosity can affect flow resistance and pump efficiency. 5. Cavitation or Aeration: Changes in fluid conditions, such as a drop in fluid pressure or an increase in fluid temperature, can lead to cavitation (the formation and collapse of vapor bubbles) or aeration (the introduction of air or gas into the fluid). These phenomena can affect pump performance and reliability. 6. Flow Reversal: Flow reversal can occur in certain situations, such as during system startup or shutdown, and can affect pump operation and the direction of flow. 7. Operational Modes: Changes in pump operating modes, such as switching between parallel or series operations in a multi-pump system, can impact fluid dynamics and overall system behavior. 8. System Changes: Modifications to the overall system design, such as changes in pipe sizes, the addition of control valves, or the introduction of new equipment, can influence fluid dynamics within the pump and the system.

Fan and Blower First Principle Failure Modes

The following table contains the first principle failure modes embedded within FactoryTalk Analytics GuardianAI for fans and blowers. Fans and blowers are a specific application of motor analytics. When monitoring a fan or blower, Factorytalk Analytics GuardianAI will provide a combination of fan/blower and motor failure modes. These may be provided as recommendations during deviation detection based on the matching frequency analysis of the deviation

Failure Mode Label	Description
Blade Misalignment	Fan blade misalignment refers to a condition in which the blades of a fan, such as those used in industrial fans, HVAC (heating, ventilation, and air conditioning)

Failure Mode Label	Description
	systems, or cooling equipment, are not properly aligned with each other or with the fan hub. This can lead to reduced airflow and efficiency loss. 1. Angular Misalignment: Angular misalignment occurs when the fan blades are not oriented correctly in relation to the fan hub or the axis of rotation. In other words, the blades are not evenly spaced around the hub, creating an angular misalignment. This can result in uneven airflow and reduced fan efficiency. 2. Parallel Misalignment: Parallel misalignment, also known as axial misalignment, occurs when the fan blades are not in the same plane as the fan hub's axis. This means that the blades are not aligned along the same plane, which can lead to imbalanced airflow and vibration. 3. Combination Misalignment: In some cases, fan blade misalignment may involve a combination of both angular and parallel misalignment, creating a more complex misalignment issue.
Blade Unbalance	Fan blade unbalance refers to an irregular distribution of mass or weight in the blades of a fan, resulting in an uneven distribution of forces as the fan rotates. This condition can lead to excessive vibration and operational problems in fan systems, including industrial fans, HVAC (heating, ventilation, and air conditioning) fans, and other types of air-moving equipment. Fan blade unbalance can occur due to various reasons, including manufacturing defects, wear and tear, erosion of blade material, damage, or the accumulation of foreign objects or debris on the blades
Blade Wear	Fan blade wear refers to the gradual deterioration or erosion of the surfaces of the blades in a fan, such as those used in industrial fans, HVAC (heating, ventilation, and air conditioning) systems, or cooling equipment, due to friction, abrasion, or other forms of material loss over time. This wear can be caused by various factors and can lead to several operational issues
Loose Blade	A loose blade in a fan refers to a condition where one or more blades of the fan assembly are not securely attached to the fan hub or rotor. This is a potentially hazardous situation that can lead to significant operational problems, safety concerns, and damage to the fan system. Loose blades can result from various factors, including manufacturing defects, wear and tear, damage to blade attachment mechanisms, improper installation, or the failure of blade fasteners or hardware.
Electrical Fault	A fan electrical fault refers to a malfunction or problem within the electrical components of a fan system, such as those found in industrial fans, HVAC (heating, ventilation, and air conditioning) fans, or cooling equipment. These electrical faults can disrupt the fan's operation, impact its performance, and pose safety risks. Fan electrical faults can occur due to various reasons, including electrical component wear, manufacturing defects, overheating, electrical surges, loose connections, insulation breakdown, or damage to electrical components.

Appendix B

Appendix B provides information about security considerations for FactoryTalk Analytics GuardianAI.

Security Considerations for FactoryTalk Analytics GuardianAI

When deploying FactoryTalk Analytics GuardianAI within operations considerations should be applied to the physical and cyber system security posture of the system. The FactoryTalk Analytics GuardianAI application is designed to run as an edge application either on FactoryTalk Edge Manager or on a client supplied edge hardware and infrastructure.

System security is a paramount tenet of overall operation success. The following document and links are being provided as guidance on best practices of how to implement system security principles within industrial automation control systems. It is of best practice for users of FactoryTalk Analytics GuardianAI to follow these practices to provide the best level of defense in depth security for their overall systems

Table 1. Security Publications

Publication Name	Description	Link
Converged Plantwide Ethernet (CPwE) Design	Converged Plantwide Ethernet Design Implementation Guide	Converged Plantwide Ethernet Design
Deploying Firewalls within CPwE Architecture	Use cases for designing, deploying, and managing industrial firewalls	Deploying Firewalls within CPwE
Deploy Identity and Mobility Services	Guidelines for protecting systems through deploying centrally managed defense in-depth security approach	Identity and Mobility Services
Secure Cloud Connectivity to CPwE	Application guide for securing cloud applications within CPwE Architecture	Secure Cloud Connectivity to CPwE
Deploy CIP Security within CPwE	Network security use cases for CPwE systems	Deploy Network Security in CPwE
Deploy CIP Security within CPwE	IEC 62443 security architecture use cases and design principles	Deploy CIP Security in CPwE
Physical Infrastructure within CPwE Architecture	Use cases for deploying robust physical infrastructure for industrial applications	Physical Infrastructure within CPwE Architecture
FactoryTalk Edge Manager	User Manual	FactoryTalk Edge Manager

Network Security and Segmentation

Network security practices within Converged Plantwide Ethernet define the usage of zones and conduits to segment assets within an industrial automation control system. When using FactoryTalk Analytics GuardianAI it is suggested to follow the CPwE Design Implementation guide (Converged Plantwide Ethernet Design) to isolate PowerFlex Drives into various zones. Also segmenting the zone where the edge node running FactoryTalk Analytics GuardianAI is a best practice. Furthermore, augmenting these zones and conduits with enhanced physical security is also a best practice as defined by Physical Infrastructure within CPwE architecture (Physical Infrastructure within CPwE Architecture). As

the CPU and memory requirements for FactoryTalk Analytics GuardianAI are imposed at runtime, it is critical that the edge node hardware selected meets the minimum requirements specified and is protected within a defense-in-depth zone. FactoryTalk Edge Manager nodes will automatically enforce the minimum requirements to run FactoryTalk Analytics GuardianAI (FactoryTalk Edge Manager).

Email Relay Server

One of the means of communication of notifications for FactoryTalk Analytics GuardianAI is a SMTP server for email notification. This SMTP server is to be provided by the user of FactoryTalk Analytics GuardianAI. It is best practice to secure this SMTP server with the defense-in-depth guidance provided by CPwE Design (Converged Plantwide Ethernet Design). Access to the FactoryTalk Analytics GuardianAI application is access-controlled, but the user of FactoryTalk Analytics GuardianAI is responsible for the security of the SMTP server.

Access to the FactoryTalk Analytics GuardianAI Application

Access to the FactoryTalk Analytics GuardianAI is privileged and access-controlled. It is up to the user of FactoryTalk Analytics GuardianAI to use strong passwords and to protect these passwords. It is also the responsibility of the user to provide appropriate access controls to the IP addresses of the applications within the facility where the application is running.

Data Integrity and Confidentiality

There is no explicit data or configuration that is shared with FactoryTalk Analytics GuardianAI. The only information exchanged between the PowerFlex Drive and FactoryTalk Analytics GuardianAI application is the three electrical phase currents and the electrical frequency. The user of the FactoryTalk Analytics GuardianAI application is responsible for protecting the container runtime environment unless run inside of FactoryTalk Edge Manager edge node (FactoryTalk Edge Manager).

Denial of Service

The FactoryTalk Analytics GuardianAI application is a small edge run application that only monitors information from PowerFlex drives to provide users insights about electromechanical anomalies and deviations. The application is intended to be run only on internal networks protected by defense-in-depth security as defined by CPwE (Converged Plantwide Ethernet Design). There is no intelligent load balancer built into this application. The user is responsible for guarding against denial-of-service attacks.