FT Analytics™ GuardianAI™

User Guide

Version 1.00.00

Rockwell Automation Publication FTGAI 95055-UM012A-EN-P

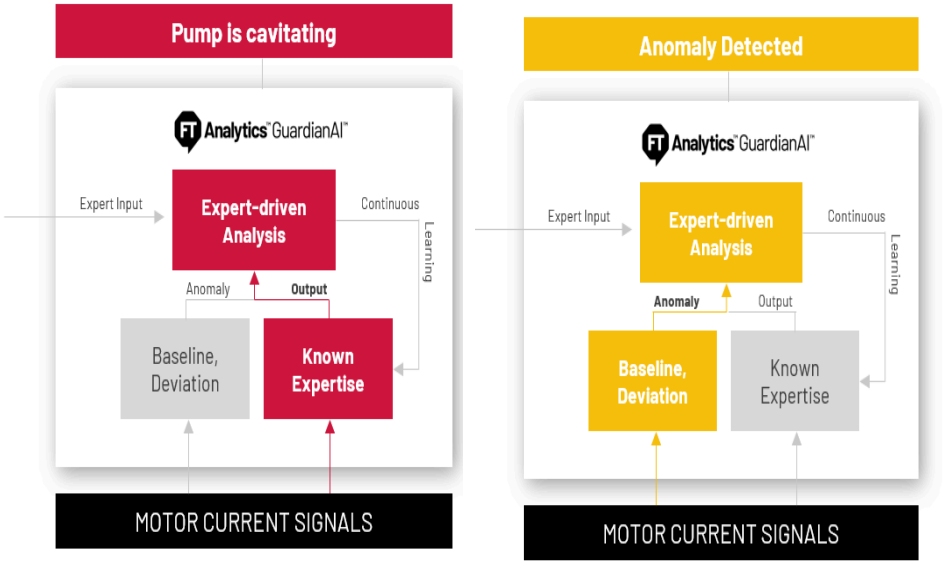
Rockwell Automation

Original Instructions

Contents

FactoryTalk Analytics GuardianAI Overview

FactoryTalk Analytics 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 assets like pumps, fans, and blowers on a plant floor. It uses device data to establish a baseline signature of each asset's behavior under normal operating conditions. Then, it monitors the assets 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, FactoryTalk Analytics 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 FactoryTalk Analytics GuardianAI machine learning engine then trains to identify the new anomaly for future encounters. The following diagram illustrates this process and the variation between a known fault and an unknown deviation.

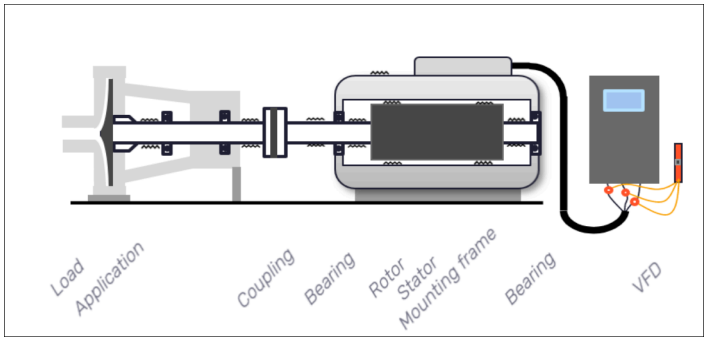


The FactoryTalk Analytics GuardianAI workflow takes a no-code approach to machine learning. As a result, a data scientist is not required to configure, deploy, or use this AI application. It is designed so that OT personnel, like maintenance engineers, controls engineers, machine operators, and plant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

The configuration workflow consists of four steps. First, the user deploys the FactoryTalk Analytics GuardianAI application on a local VM or edge device. Then, the user adds the device acting as the sensor. Finally, the user inputs the identifying information about the asset being monitored (pump, fan, blower, or motor). After that, the user is ready to start training the model to establish the baseline.

FactoryTalk Analytics GuardianAI is providing premier integration with PowerFlex® 755, 755TL, 755TR, 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 asset types: pumps, fans, and blowers. The application is designed to work with single-drive and motor applications. Given its adaptive nature, FactoryTalk Analytics 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 an asset



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

Pumps
- ✓ Impeller Unbalance
- ✓ Blade Fault
- ✓ Cavitation
- ✓ Viscosity Changes
- ✓ Shaft Misalignment
- ✓ Change in Fluid Dynamics

Fans and Blowers
- ✓ Blade Misalignment
- ✓ Blade Unbalance
- ✓ Blade Wear
- ✓ Loose Blade
- ✓ Electrical Fault
- ✓ Motor Fault
- ✓ Shaft Misalignment
- ✓ Fan Bearing Fault

Motor Analytics
- ✓ Unbalance
- ✓ Shaft Misalignment
- ✓ Loose Structural Mounting (Soft Foot)
- ✓ Mechanical Looseness
- ✓ Rotor Rub
- ✓ Ball Bearing Fault
- ✓ Inner Race Bearing Fault
- ✓ Outer Race Bearing Fault
- ✓ Bearing Cage Fault

Key Features

- **No Code** FactoryTalk Analytics 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** FactoryTalk Analytics 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. FactoryTalk Analytics GuardianAI trains and runs right at the edge providing real-time predictions and minimizing the total cost of ownership.

Getting Started with FactoryTalk Analytics GuardianAI

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

User Interface

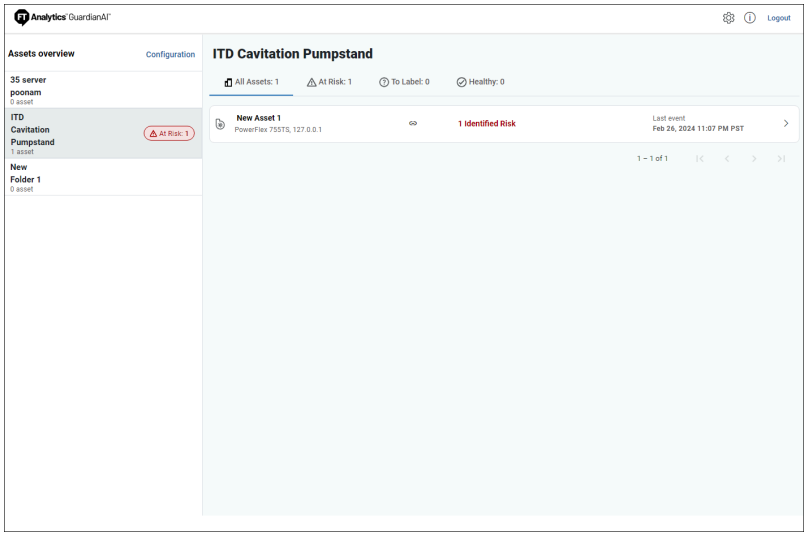
This topic will help you get familiar with the FactoryTalk Analytics GuardianAI user interface.

Monitoring Workspace

The monitoring workspace is displayed in the following figure, which is used to provide quick access to the overall status of the assets monitored by FactoryTalk Analytics GuardianAI.

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

Figure 2. Asset Monitoring Workspace



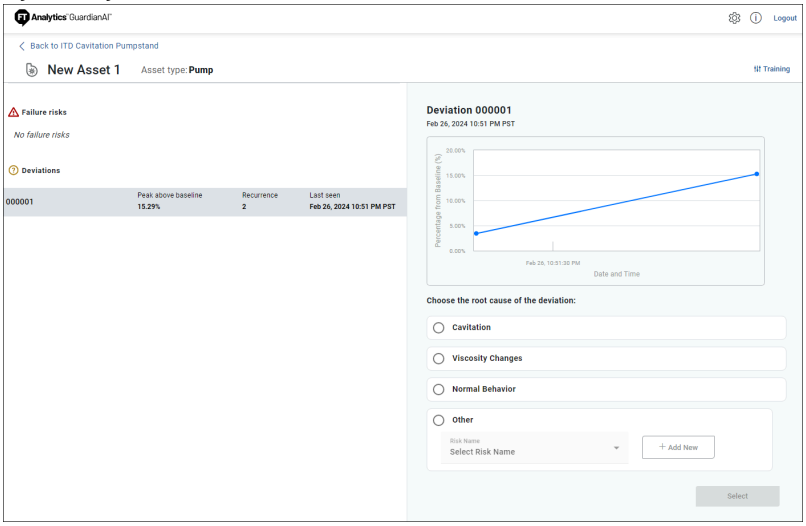
Single Asset View

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

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

The following image displays a deviation. Once displayed, the deviation will have a set of first principle recommendations for the user to select from. In the following example, FactoryTalk Analytics GuardianAI detected a deviation with a signature matching pump cavitation or a fluid viscosity change. If the user believes that the deviation is incorrect, they have the ability to select normal operation or create a new label.

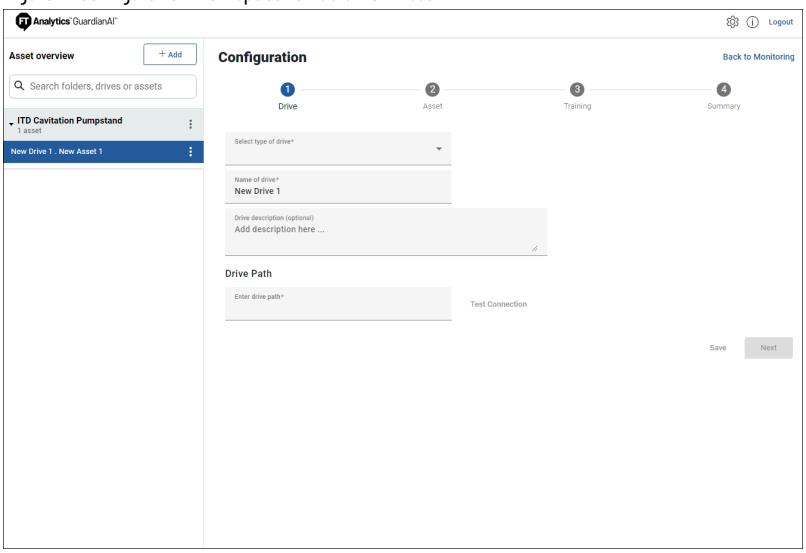
Figure 3. Single Asset View with Deviation Detected



Configuration Workspace

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

Figure 4. Configuration Workspace to Add a New Asset

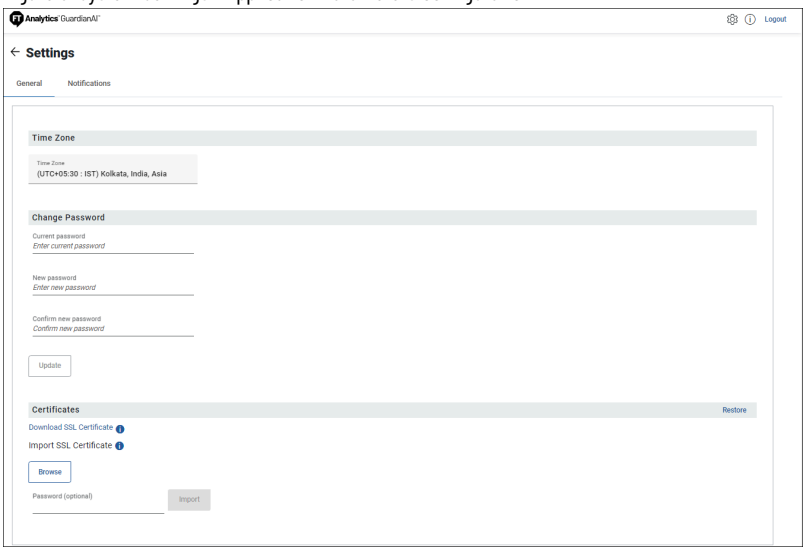


System Settings Workspace

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

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

Figure 5. System Settings - Application Parameters Configuration

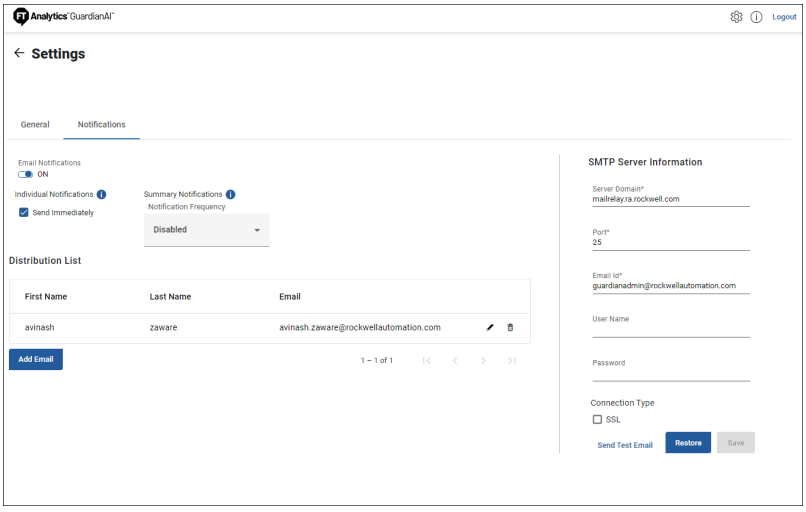


Notifications

The notification settings enable FactoryTalk Analytics 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 Pre-Requisites and Considerations

High Speed Trend Configuration

- FactoryTalk Analytics GuardianAI utilizes the high-speed trend function provided by the variable frequency drives. This function will not be available for other application usage while FactoryTalk Analytics GuardianAI is training and monitoring the asset. A user should stop training and monitoring with FactoryTalk Analytics GuardianAI to release usage of the High-Speed data trend.
- The user needs to ensure that their target drive has High Speed Trend configured for Active Mode 0 (8 buffers, 4096 samples).

Figure 7. High-speed Test Configuration

NOTE: This setting can be configured using the High-Speed Trend Wizard in Logix Designer or Connected Component Workbench

- 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 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 FactoryTalk Analytics GuardianAI is training and monitoring an asset may impact FactoryTalk Analytics 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:

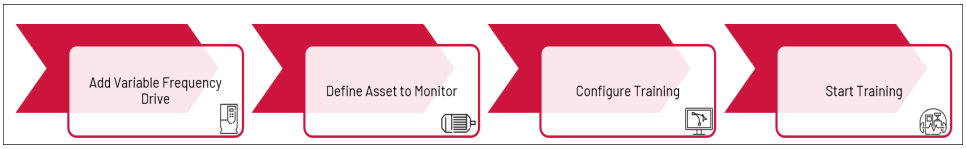
- PowerFlex 755T and 6000T
  - [10:0381] Testpoint REAL 1
  - [10:0384] Testpoint REAL 2
  - [10:0387] Testpoint REAL 3
- PowerFlex 755
  - [00:0971] Testpoint Fval 1
  - [00:0975] Testpoint Fval 2
  - [00:0979] Testpoint Fval 3

Drive Firmware Version Support

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

Adding a new Drive and Asset to Monitor

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



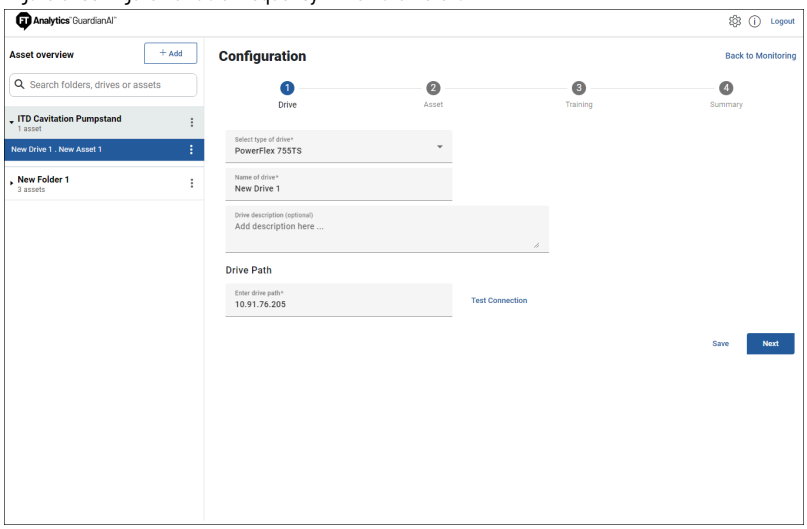
1. Add and configure the variable frequency drive. Supported drives include Powerflex 755, 755TS/TL/TM/TR and 6000T.
2. Define the asset to monitor (pump, fan, blower, motor for other asset types).
3. Configure Training (Define the minimum and maximum speed of the application)
4. Start Training Process

Configuring Drive

To add a new drive the user needs to fill out the following fields:

- **Drive Type**: 755, 755TM, 755TR, 755TL, 755TS, 6000T
- **Name**: provide a unique name for the drive
- **Description** (optional)

Figure 8. Configure Variable Frequency Drive Parameters

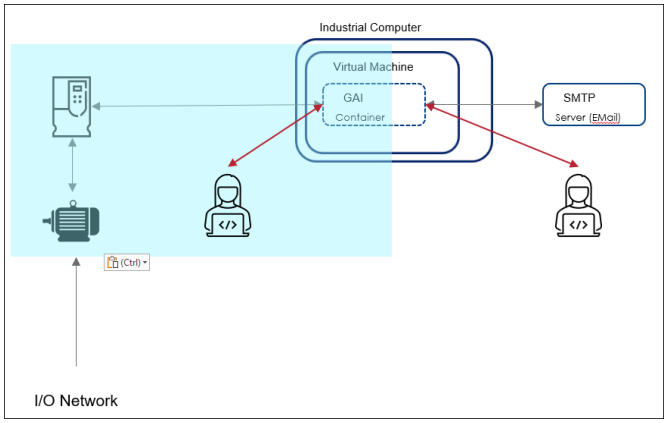


The drive path depends on the network configuration of the drive and the PC hosting FactoryTalk Analytics GuardianAI. If both are on the same network, the drive can be accessible directly via an IP Address. For this scenario the user can input the IP address of the drive.

IP Address format example: 192.168.1.10

The following illustration depicts the PC that hosts FactoryTalk Analytics GuardianAI and drive existing on the same network location.

Figure 9. Network Illustration of Edge PC and Drive on the Same Network

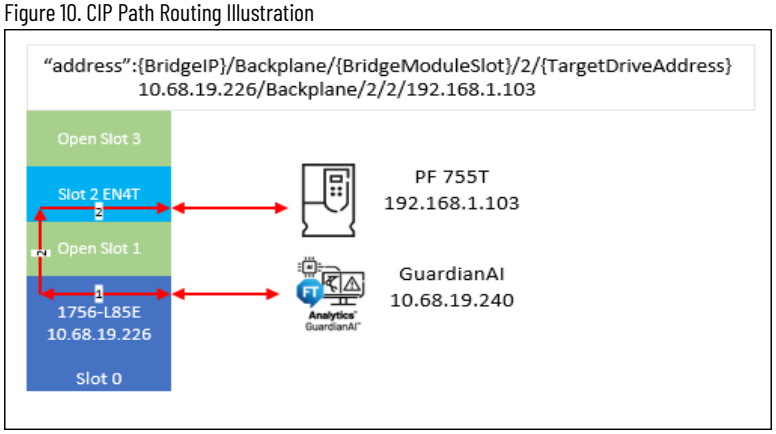


The more likely scenario is the PC that hosts FactoryTalk Analytics GuardianAI is on the same network layer as the controller. In this case, the user needs to input the full CIP path mapping from the controller to the drive.

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

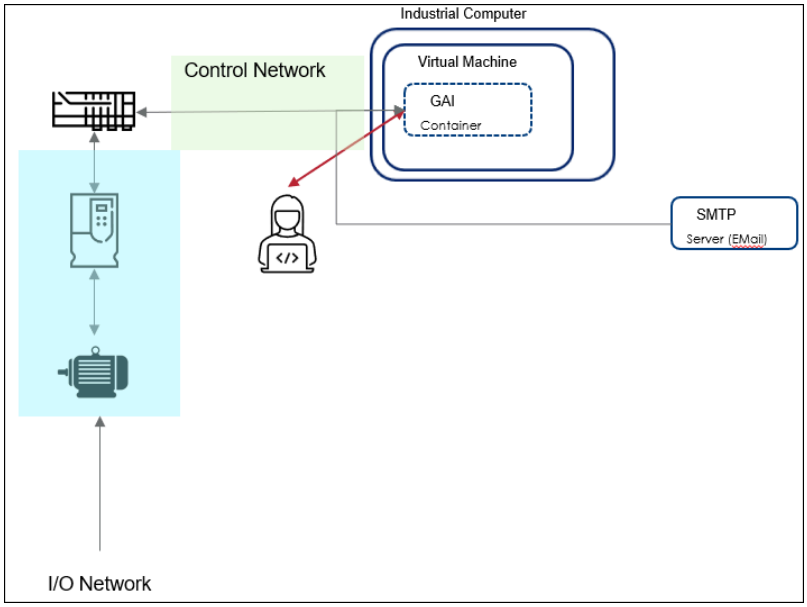
CIP Path Example: 11.70.20.214/Backplane/2/2/192.168.1.103

Figure 10. CIP Path Routing Illustration



The following illustration depicts the PC that hosts FactoryTalk Analytics GuardianAI existing on the control network and the variable frequency drive (VFD) on a subnet.

Figure 11. Network Illustration of Edge PC on the Control Network and Drive on a Subnet



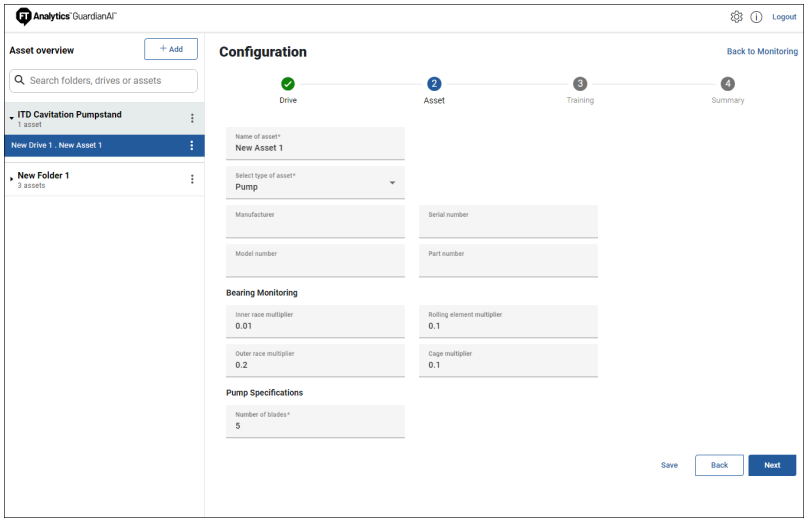
NOTE: Test the connection to the drive to ensure the drive is connected and FactoryTalk Analytics GuardianAI can successfully establish and validate the connection.

Configuring Asset

To add a new drive the user should provide the following information:

- Asset Name: Provide a unique name for an asset.
- Asset Type: Pump, Fan, Blower, Motor (used for other asset types)
- Manufacturer (optional)
- Serial number (optional)
- Model number (optional)
- Part number (optional)

Figure 12. Configure Asset Parameters

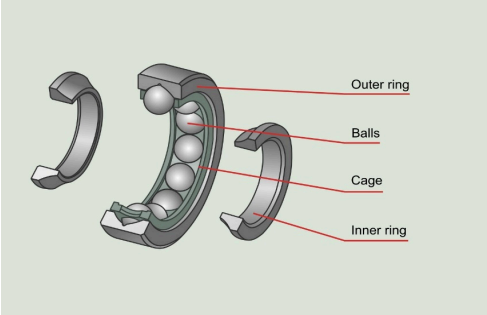


Bearing Monitoring

The bearing dimensions are used by the FactoryTalk Analytics GuardianAI algorithm to provide first principle failure mode recommendations. The failure modes included with 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, FactoryTalk Analytics 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 13. 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.

Pump of Fan Specifications

The Number of Blades field is only displayed for the pump or fan selection in the asset type drop down.

- **Number of Blades**: integer number entry only

Configuring Asset Training

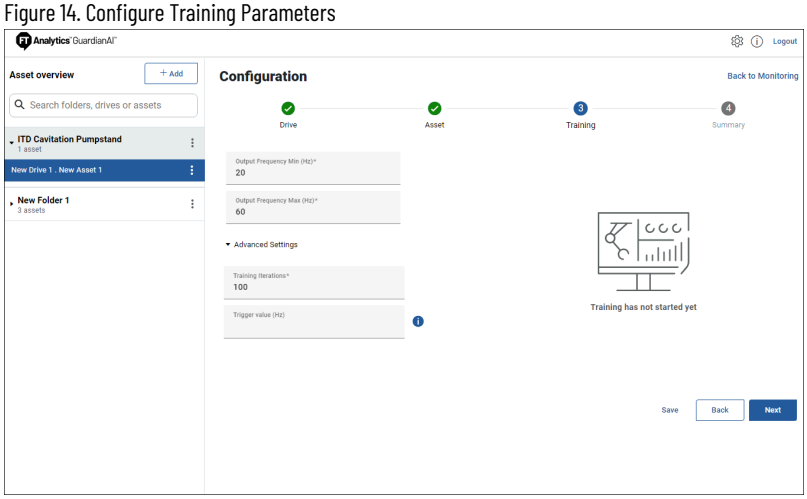
- **Output Frequency Min (Hz)**: Minimum VFD command frequency of the application
- **Output Frequency Max (Hz)**: Maximum VFD command frequency of the application

Advanced Settings

- **Training Iterations (Default 100)**: The number of data trends received from the variable frequency drives from FactoryTalk Analytics 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 taken to train the baseline will be between 11-18 minutes for each half hertz increment of the operation frequency.
- **Trigger Value Hz (Default Empty)**: Advanced trigger configured for the drive high speed trend object. The value set will configure the drive to only send data to FactoryTalk Analytics GuardianAI for training/monitoring when the drive is operating 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 FactoryTalk Analytics GuardianAI on pumps, fans, and blowers.

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

Figure 14. Configure Training Parameters

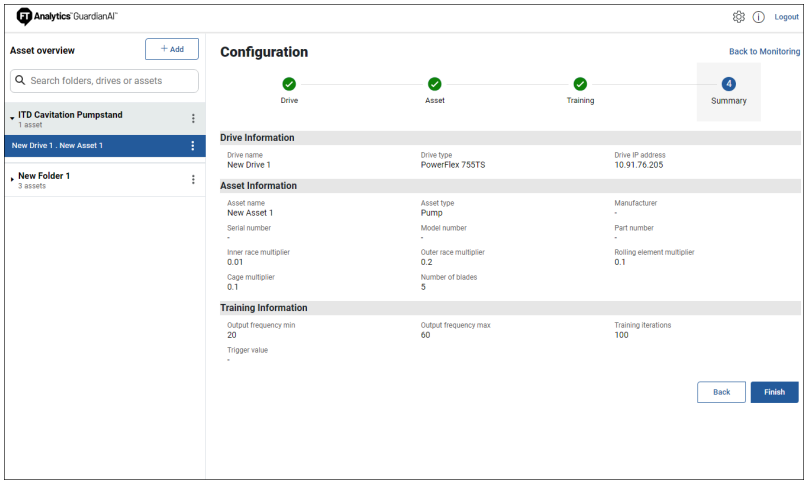


Configuration Summary

After completing the steps for drive, asset, and training configuration, FactoryTalk Analytics 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, the user will be able to save and finish the configuration of the new asset.

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

Figure 15. Configuration Summary and Validation



Training the Asset Baseline

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

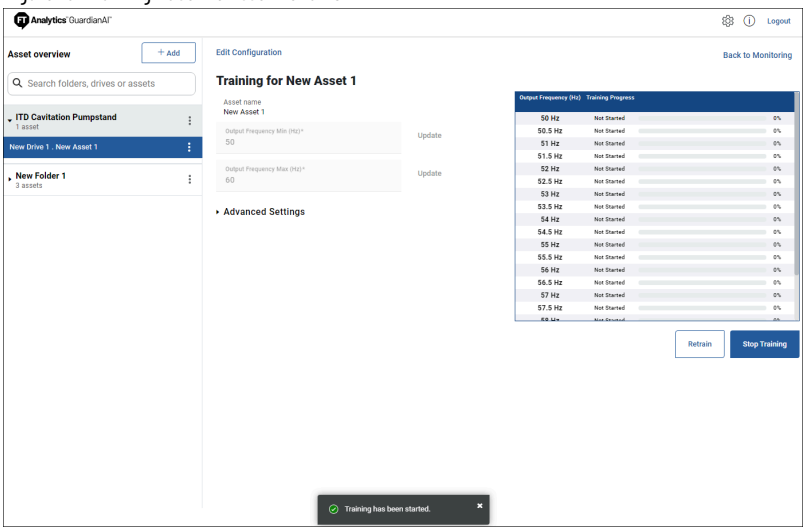
Start Training

After clicking **Start Training**, 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. 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 asset is in training, the user will not be able to edit the configuration of that asset. To make any edits, the user should click the stop training button.

Figure 16. Training Baseline Asset Behavior

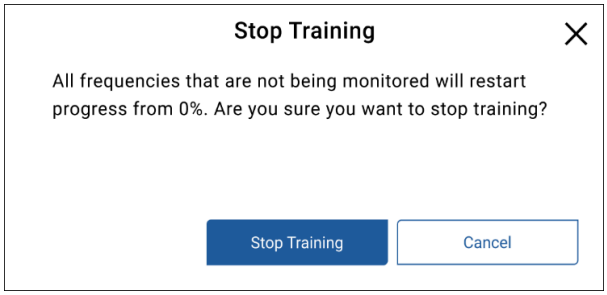


Stop Training and Monitoring

Stopping training will also stop 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 in-progress buckets reset and confirm the action.

Figure 17. Stop Training Dialog Box



The user should stop training to make any edits to the drive configuration.

Re-train Asset

Re-training an asset can be important if a major physical change is made to the system. An example might be replacing the motor or full re-alignment of a coupling. FactoryTalk Analytics GuardianAI starts the training process under normal conditions, but it is possible there was already existing degradation at the time 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 FactoryTalk Analytics GuardianAI will view normal operation as anomalous behavior. If too many false positives are detected after a major maintenance event, then FactoryTalk Analytics GuardianAI should be re-trained to acquire a new baseline of the asset's behavior.

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 FactoryTalk Analytics GuardianAI. FactoryTalk Analytics GuardianAI 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 18. Deviation to Failure Risk Workflow

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

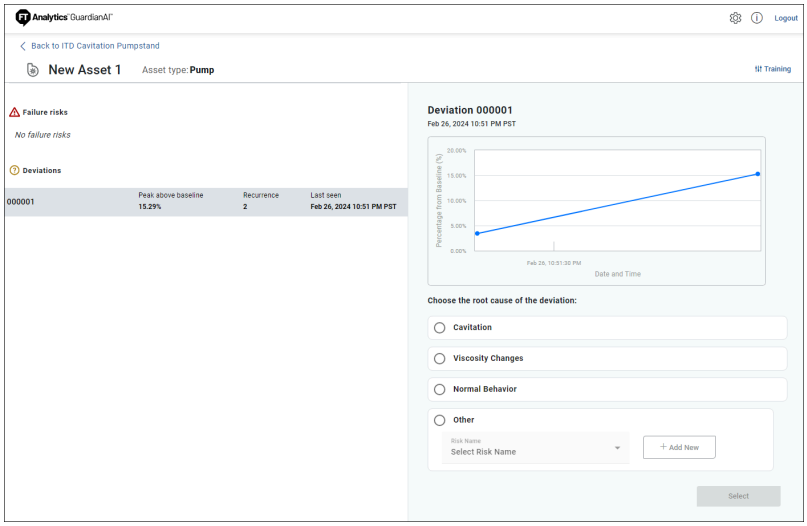
1. A deviation is detected with associated first principle recommendations.
2. The user selects between the first principle, normal operation, or creates a new label.
3. Once the detected deviation is labeled, the deviation will move to a failure risk.
4. The user should select and resolve a failure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

Labeling Deviations

All new anomalies detected by FactoryTalk Analytics 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**: FactoryTalk Analytics GuardianAI may incorrectly detect the deviation. A user can select normal behavior to train FactoryTalk Analytics GuardianAI to recognize the detected pattern as normal.
- **Other**: A drop-down will display other labels stored in the FactoryTalk Analytics GuardianAI database to select from. The user can also choose to create a new label for the deviation

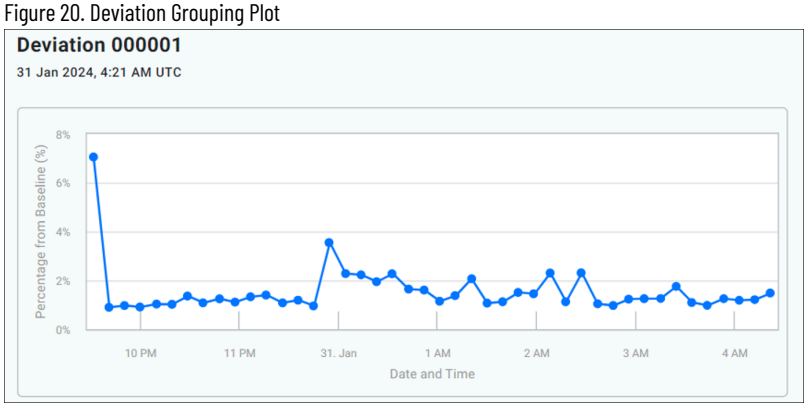
Figure 19. Deviation Detection and Grouping



Deviation Grouping

FactoryTalk Analytics GuardianAI 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.

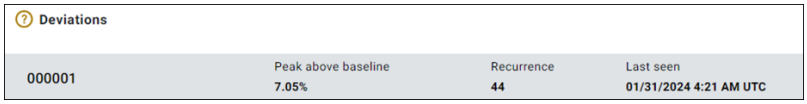
Figure 20. Deviation Grouping Plot



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 21. Deviation Summary



First Principle Failure Mode Recommendations

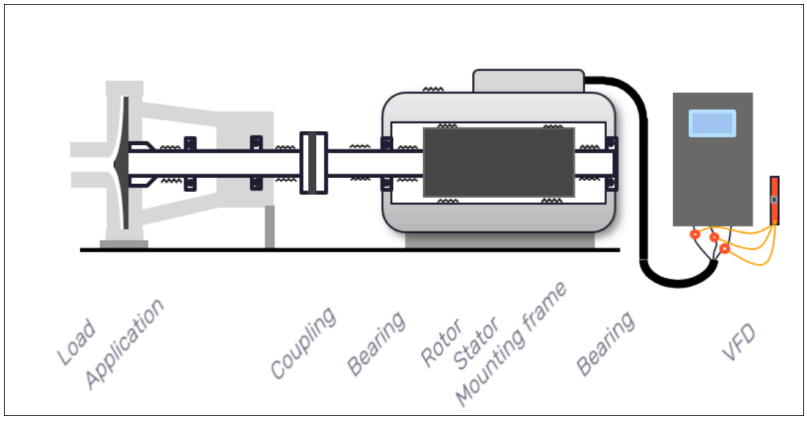
When providing first principle recommendations, some frequencies may overlap resulting in several suggestions made by FactoryTalk Analytics GuardianAI.

For motor analytics, FactoryTalk 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 22. 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, FactoryTalk Analytics GuardianAI will provide first principle recommendations for the specific application and the motor analytics. As illustrated below, the analysis from FactoryTalk Analytics GuardianAI is inclusive of the motor, coupling, and Load application.

Figure 23. 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 FactoryTalk Analytics 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 asset may be required.

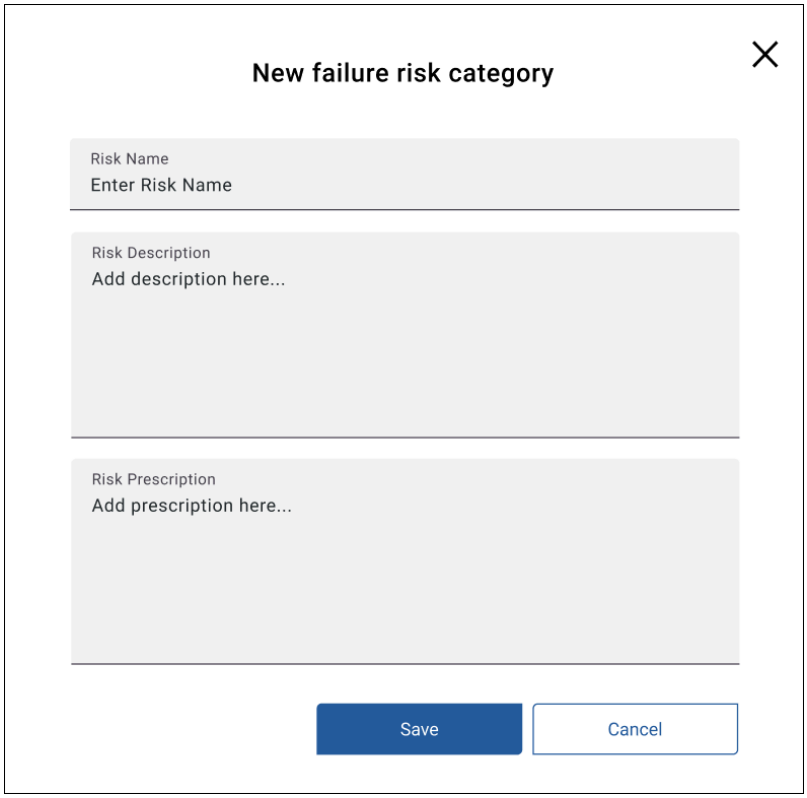
Creating a New Deviation Label

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 24. Other & Add New Deviation Label

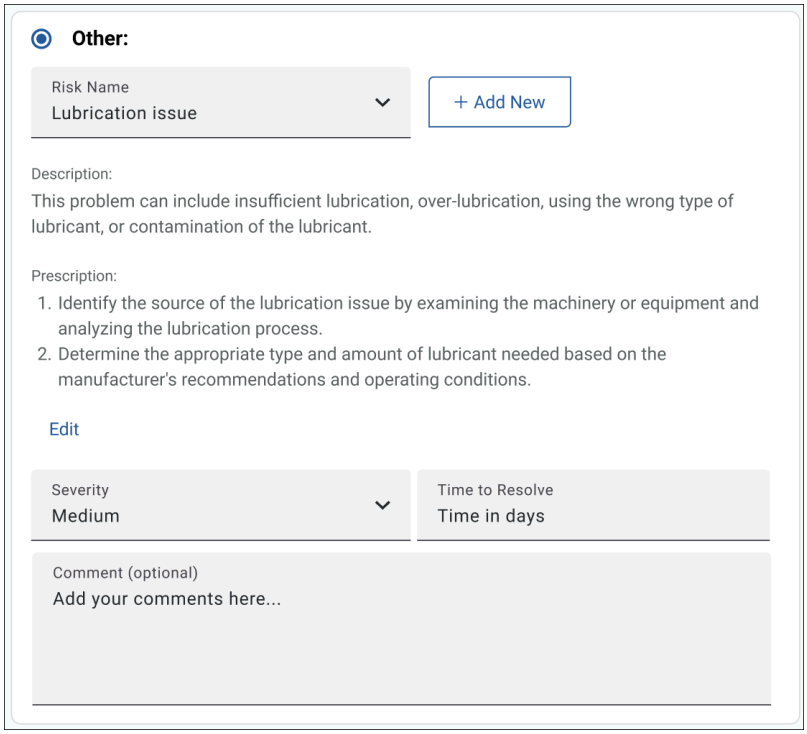
A dialogue box is displayed with the fields to create the new failure Risk label. The label includes the name, descriptions, and prescription (optional).

Figure 25. Creating a New Failure Risk



Upon creating the new label, the user can associate severity and recommended time to resolve the deviation.

Figure 26. Severity and Time to Resolve



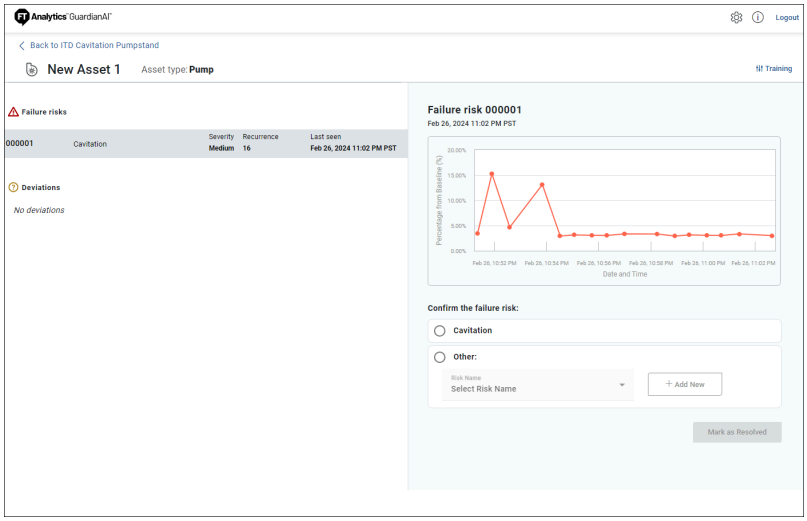
Detecting Failure Risks

Failure risks are deviations that have been labeled and confirmed by a user. If an anomaly is detected again, FactoryTalk Analytics GuardianAI will automatically display it as a failure 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. FactoryTalk Analytics GuardianAI will bring back the failure risk if the signature is detected again.

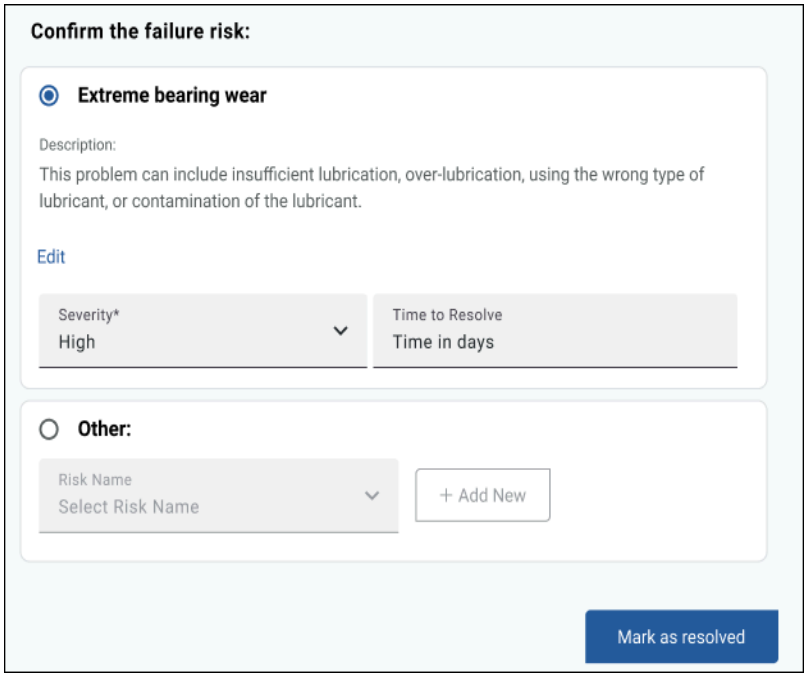
Figure 27. Failure Risk Detection and Grouping



Resolving Failure Risks

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

Figure 28. Resolve a Failure Risk

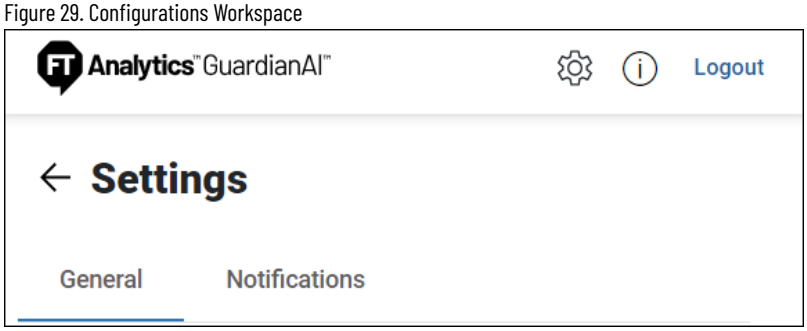


A user can also change the failure risk label and create a new one by using the same steps illustrated in the deviation workflow section on Creating a New Deviation Label. The user can select the **Other** option and either choose a label from the drop-down or create a new failure risk label.

Configuration Workspace

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

Figure 29. Configurations Workspace



Notifications

FactoryTalk Analytics GuardianAI can provide 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 edge node hosting FactoryTalk Analytics 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

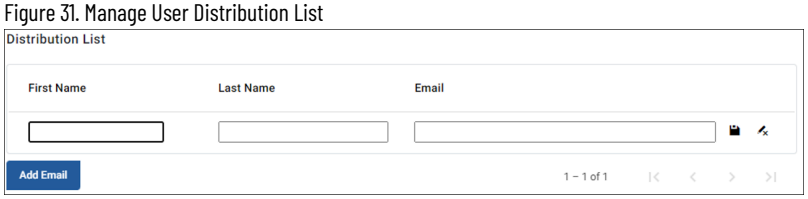
Figure 30. SMTP Server Configuration

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 31. 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 32. Edit a User in the Distribution List

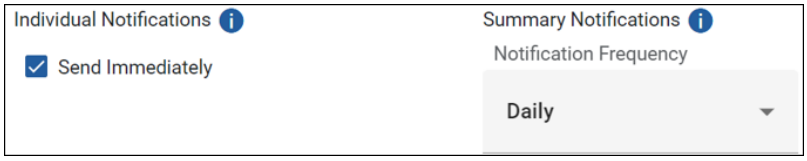
Removing a User from the Distribution List

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 33. 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

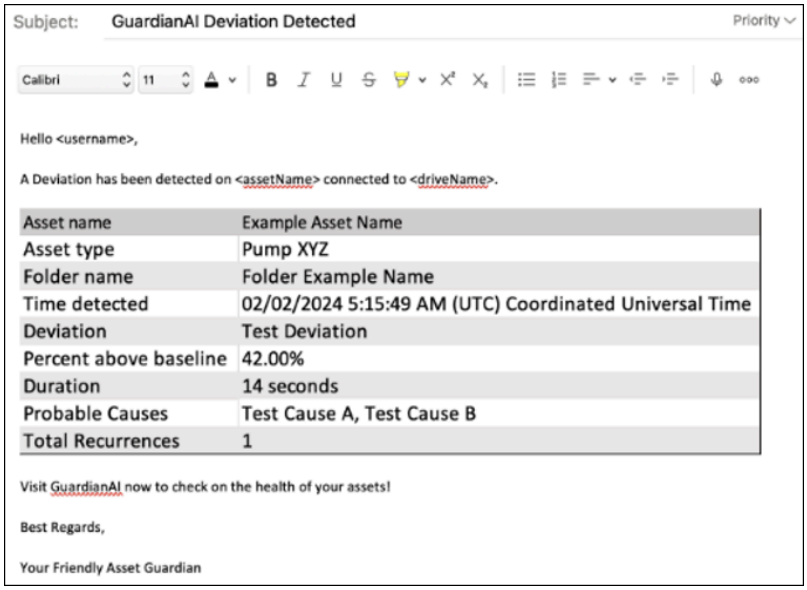
This topic describes the email templates for single event notification and summary notification.

Single Event Notification

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

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

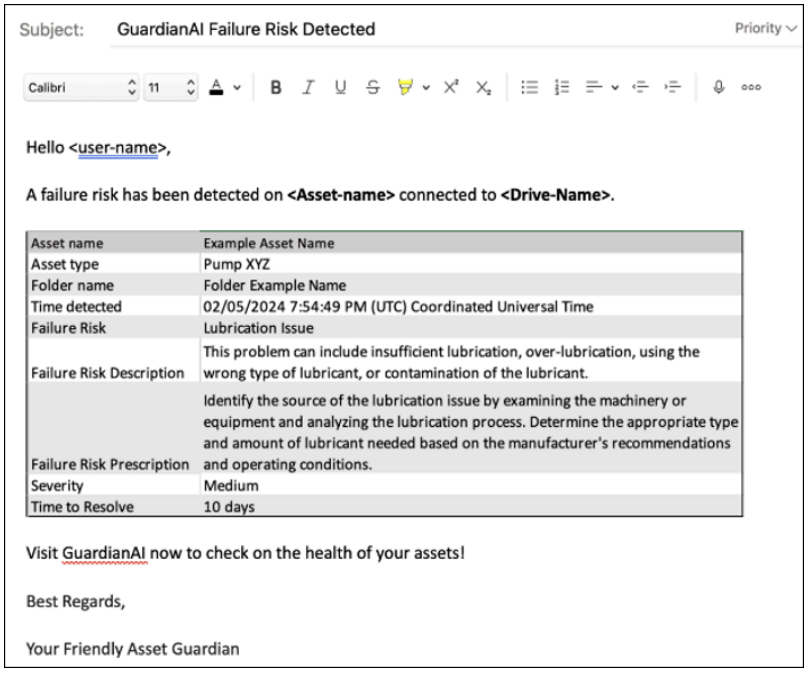
Figure 34. Example of Deviation Notification Email



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

Figure 35. Example of Failure Risk Notification Email

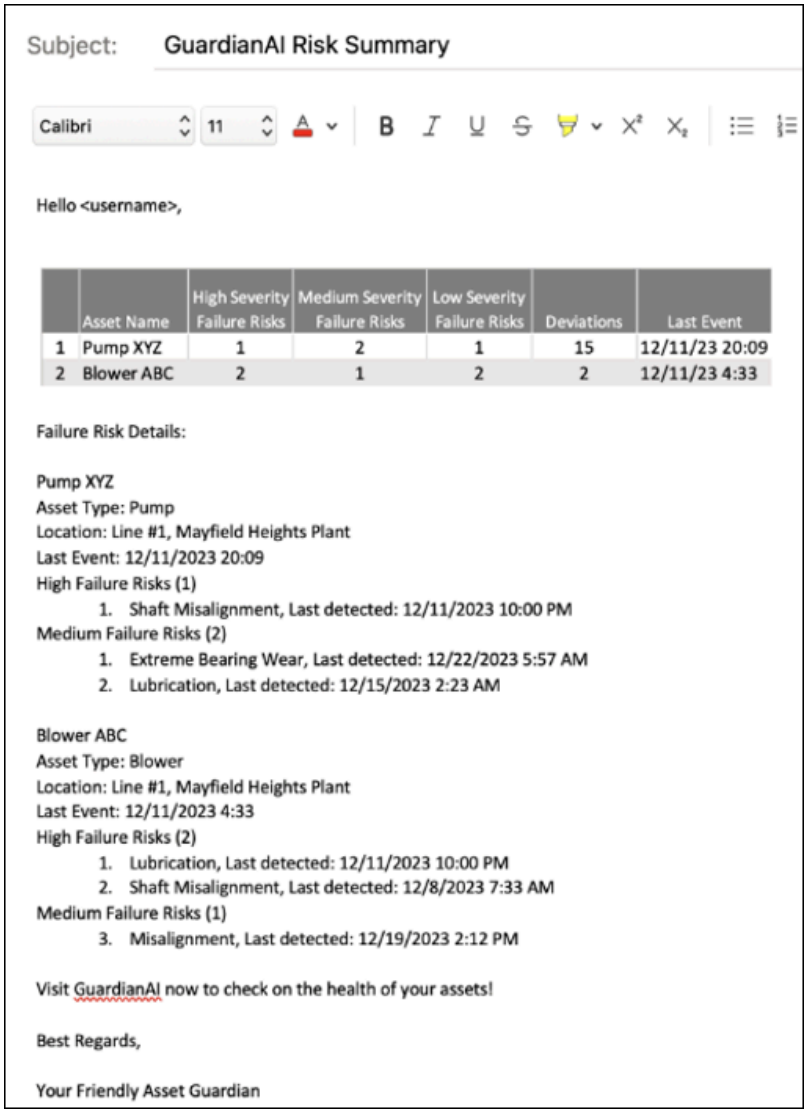


- **Asset Name**: Name of the asset given during the first-time configuration.
- **Asset Type**: Pump, Fan, Blower, or Motor Analytics.
- **Folder Name**: The folder name containing the drive and asset combination.
- **Time Detected**: The time at which the event was detected based on the local time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

Summary Notification

The summary notification provides a high-level table regarding all unlabeled deviations and unresolved failure risks for all assets monitored by FactoryTalk Analytics GuardianAI. The table rows will show the asset names, with one row dedicated to each asset. 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 36. Summary Notification



Subject: GuardianAI Risk Summary

Calibri 11

Hello <username>,

	Asset Name	High Severity Failure Risks	Medium Severity Failure Risks	Low Severity Failure Risks	Deviations	Last Event
1	Pump XYZ	1	2	1	15	12/11/23 20:09
2	Blower ABC	2	1	2	2	12/11/23 4:33

Failure Risk Details:

Pump XYZ
Asset Type: Pump
Location: Line #1, Mayfield Heights Plant
Last Event: 12/11/2023 20:09
High Failure Risks (1)
1. Shaft Misalignment, Last detected: 12/11/2023 10:00 PM
Medium Failure Risks (2)
1. Extreme Bearing Wear, Last detected: 12/22/2023 5:57 AM
2. Lubrication, Last detected: 12/15/2023 2:23 AM

Blower ABC
Asset Type: Blower
Location: Line #1, Mayfield Heights Plant
Last Event: 12/11/2023 4:33
High Failure Risks (2)
1. Lubrication, Last detected: 12/11/2023 10:00 PM
2. Shaft Misalignment, Last detected: 12/8/2023 7:33 AM
Medium Failure Risks (1)
3. Misalignment, Last detected: 12/19/2023 2:12 PM

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

Best Regards,

Your Friendly Asset Guardian

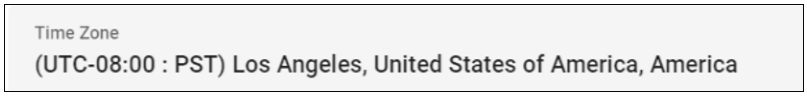
General Settings

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 37. General Settings - Time zone Configuration

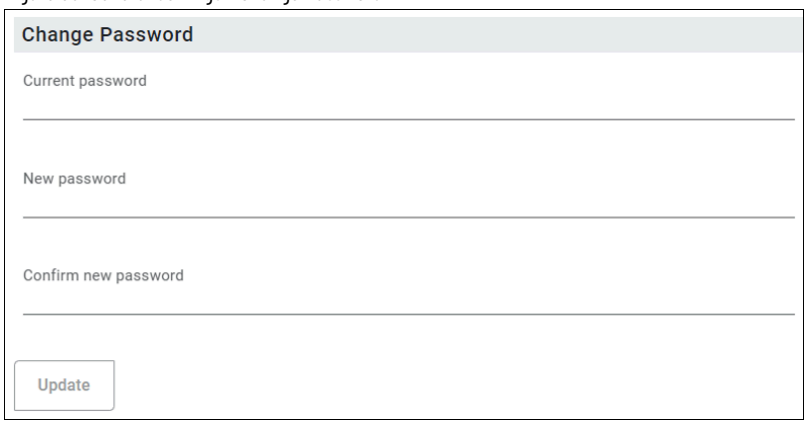


Time Zone
(UTC-08:00 : PST) Los Angeles, United States of America, America

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.

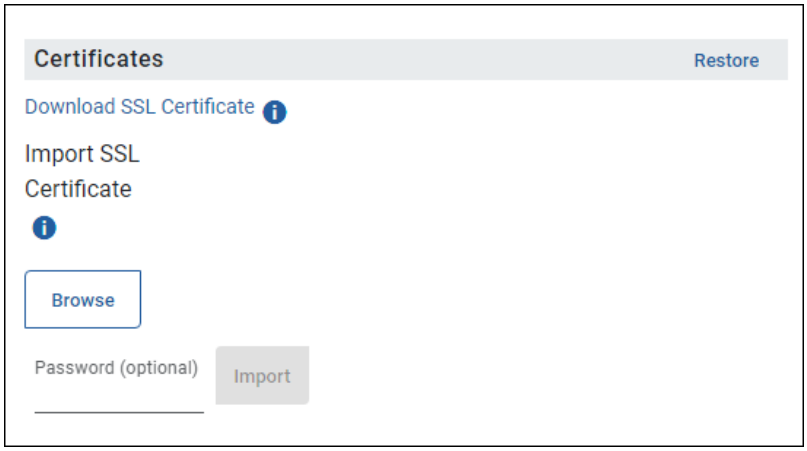
Figure 38. General Settings - Change Password



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 39. General Settings - Import SSL Certificate



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.