

ICS Blue Team Documentation

2024

CYBERFORCE COMPETITION®

CONTENTS

CONNECTIVITY	2
PLC	2
CNC/HMI	2
ENERGIA VENTOSA INDUSTRIAL CONTROL SYSTEM MANUAL	2
REGISTERS (2048-2090) AND COILS (0000-0005)	2
SYSTEM ALERTS AND THRESHOLDS	3
PLC	3
HMI	5
ENERGIA VENTOSA ENERGY GRID MAP	20
TROUBLESHOOTING COMMON ISSUES	22

Please Note:

Both the CnC and PLC VMs are within the Assume Breach infrastructure and should not be altered prior to the competition or unless provided direct instruction from Red Team.

CONNECTIVITY

PLC

Ubuntu 22.04

10.0.x.140

blueteam : BlueTeam2024!

PLC - :502

CNC/HMI

Windows Server 2016

10.0.x.141

blueteam : BlueTeam2024!

Ignition Gateway - :8088

BlueTeam : BlueTeam2024!

For more information about Ignition please visit:

<https://www.inductiveuniversity.com/courses/ignition/ignition-overview/8.1>

ENERGIA VENTOSA INDUSTRIAL CONTROL SYSTEM MANUAL

REGISTERS (2048-2090) AND COILS (0000-0005)

```
Turbine 1 Coil (0000)= turbine1_coil AT %QX0.0 : BOOL
Turbine 2 Coil (0001)= turbine2_coil AT %QX0.1 : BOOL
Turbine 3 Coil (0002)= turbine3_coil AT %QX0.2 : BOOL
Turbine 4 Coil (0003)= turbine4_coil AT %QX0.3 : BOOL
Manual Override Coil (0004)= man_over AT %QX0.4 : BOOL
Turbine 1 Direction (2048)= turbine1_direction AT %MD0 : REAL
Turbine 2 Direction (2050)= turbine2_direction AT %MD1 : REAL
Turbine 3 Direction (2052)= turbine3_direction AT %MD2 : REAL
Turbine 4 Direction (2054)= turbine4_direction AT %MD3 : REAL
Turbine 1 Out (2056)= turbine1_out AT %MD4 : REAL
Turbine 2 Out (2058)= turbine2_out AT %MD5 : REAL
Turbine 3 Out (2060)= turbine3_out AT %MD6 : REAL
Turbine 4 Out (2062)= turbine4_out AT %MD7 : REAL
Turbine 1 Generation (2064)= turb1_gen AT %MD8 : REAL
Turbine 2 Generation (2066)= turb2_gen AT %MD9 : REAL
Turbine 3 Generation (2068)= turb3_gen AT %MD10 : REAL
Turbine 4 Generation (2070)= turb4_gen AT %MD11 : REAL
Turbine Output (2072)= turbine_output AT %MD12 : REAL
Perfect Output (2074)= perfect_output AT %MD13 : REAL
PreTransformerV StepUp (2076)= pre_transf_stepupV AT %MD14 : REAL
PostTransformerV StepUp (2078)= post_transf_stepupV AT %MD15 : REAL
PreTransformerC StepUp (2080)= pre_transf_stepupC AT %MD16 : REAL
```

```
PostTransformerC StepUp (2082)= post_transf_stepupC AT %MD17 : REAL
Wind Speed (2084)= wind_speed AT %MD18 : REAL
Wind Direction (2086)= wind_direction AT %MD19 : REAL
Alert 1 (2088)= alert1 AT %MD20 : REAL
Alert 2 (2090)= alert2 AT %MD21 : REAL
```

SYSTEM ALERTS AND THRESHOLDS

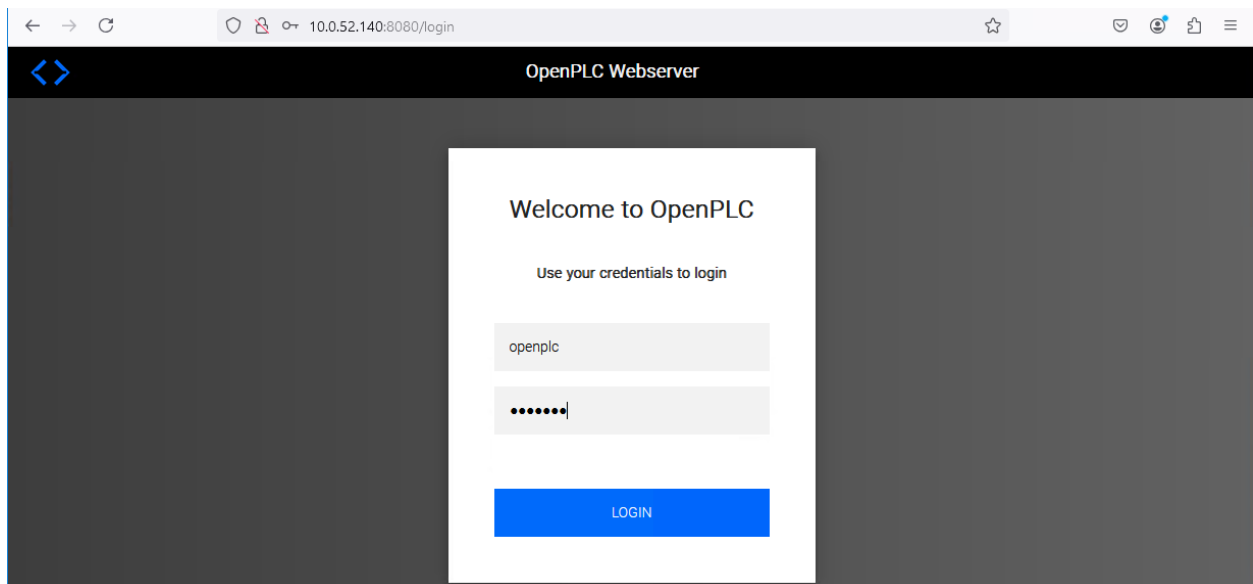
If the wind speed is below 8.0 mph, the turbine will not start.

If the wind speed is above 55.0 mph, the turbine will shutdown.

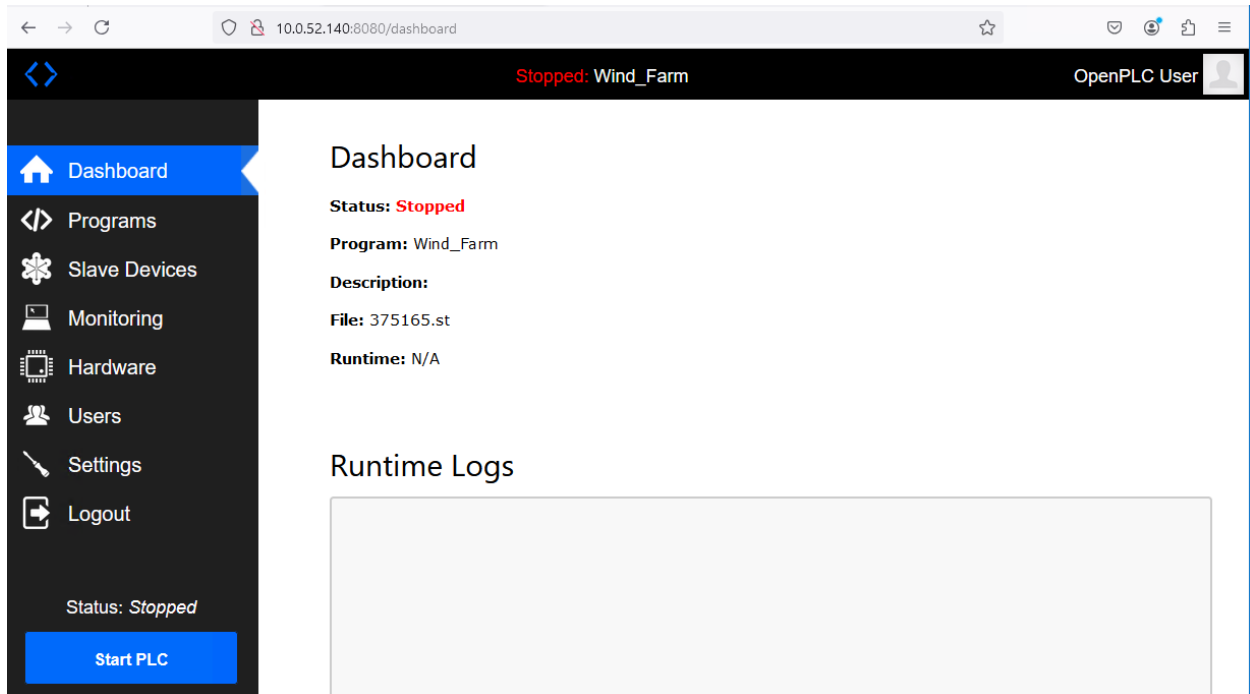
Turbine generation output is determined by the wind speed, wind direction, and turbine direction.

PLC

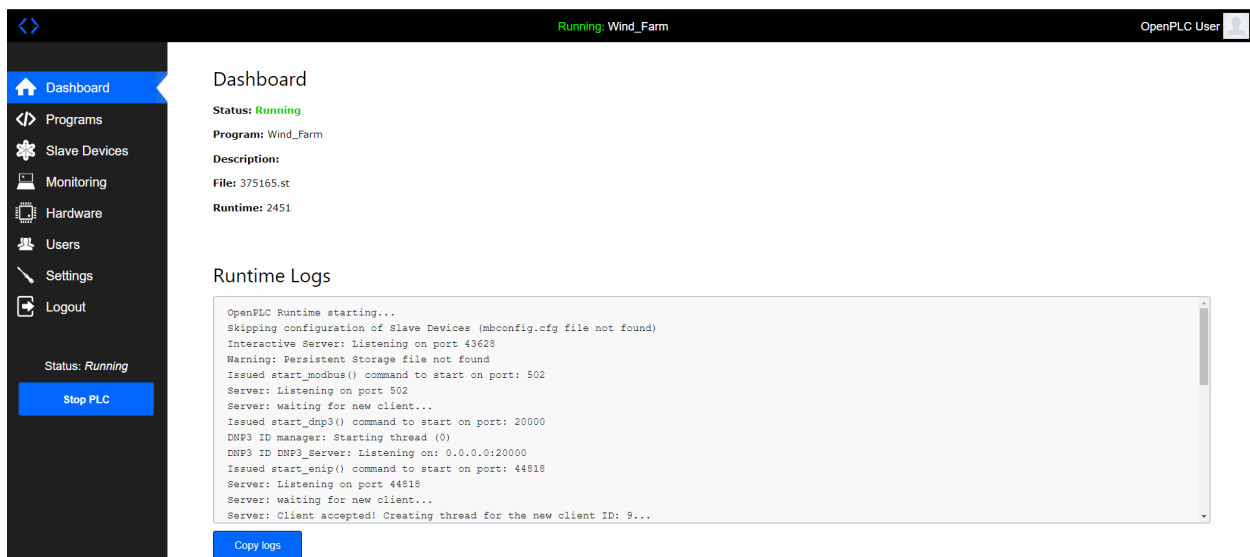
First, we must begin by starting the PLC, by going to <plc-ip>:8088. Here you will see the OpenPLC web page prompt. The credentials are openplc : openplc



Once logged in you should see the dashboard, from here you can click the blue button “Start PLC”. This will initialize the Wind-Farm PLC Program.



Below is what you should see after the PLC program has started completely.



Below is the monitoring display where you can see all of the coils and registers associated with the PLC program along with their locations and current values.

<>

Running: Wind_Farm

OpenPLC User

Dashboard

Programs

Slave Devices

Monitoring

Hardware

Users

Settings

Logout

Status: Running

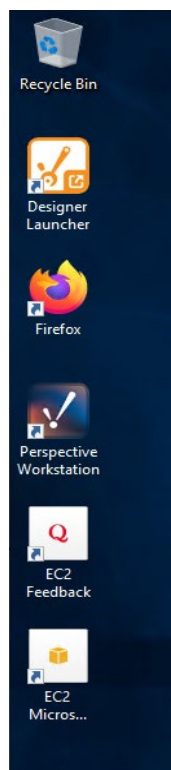
Stop PLC

Monitoring

Refresh Rate (ms): 100 Update

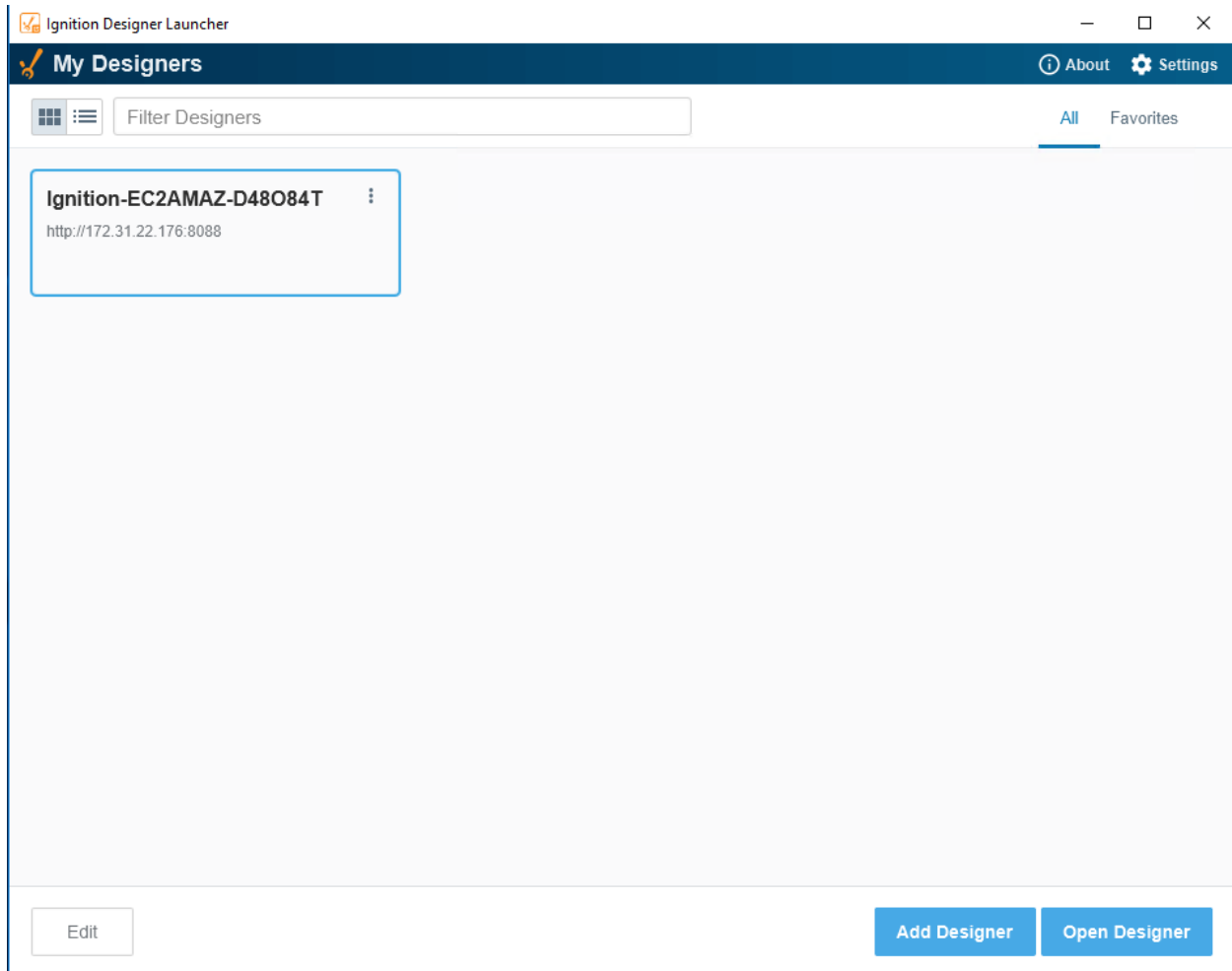
Point Name	Type	Location	Forced	Value
turbine1_coil	BOOL	%QX0.0	No	FALSE
turbine2_coil	BOOL	%QX0.1	No	FALSE
turbine3_coil	BOOL	%QX0.2	No	FALSE
turbine4_coil	BOOL	%QX0.3	No	FALSE
man_over	BOOL	%QX0.4	No	FALSE
turbine1_direction	REAL	%MD0	No	30.0000
turbine2_direction	REAL	%MD1	No	92.0000

HMI

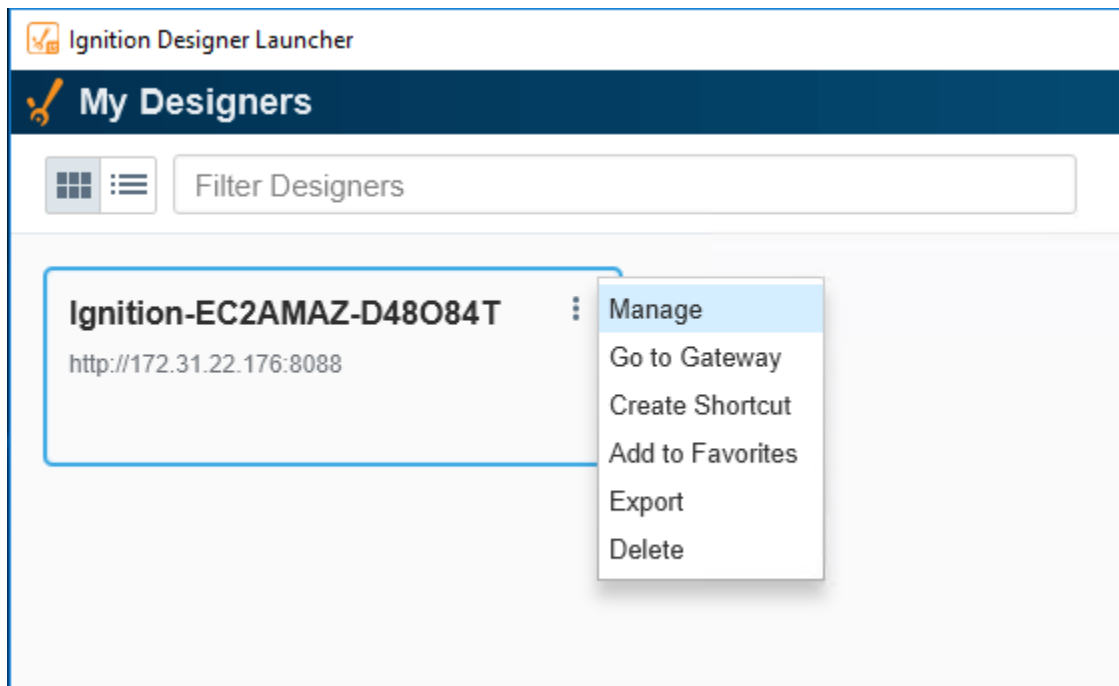


On the Desktop of the Windows 2016 CnC there are two icons designated for the Ignition HMI. Designer Launcher, launches the Ignition Designer application and the Perspective Workstation icon launches the HMI Perspective engineering workstation viewer.

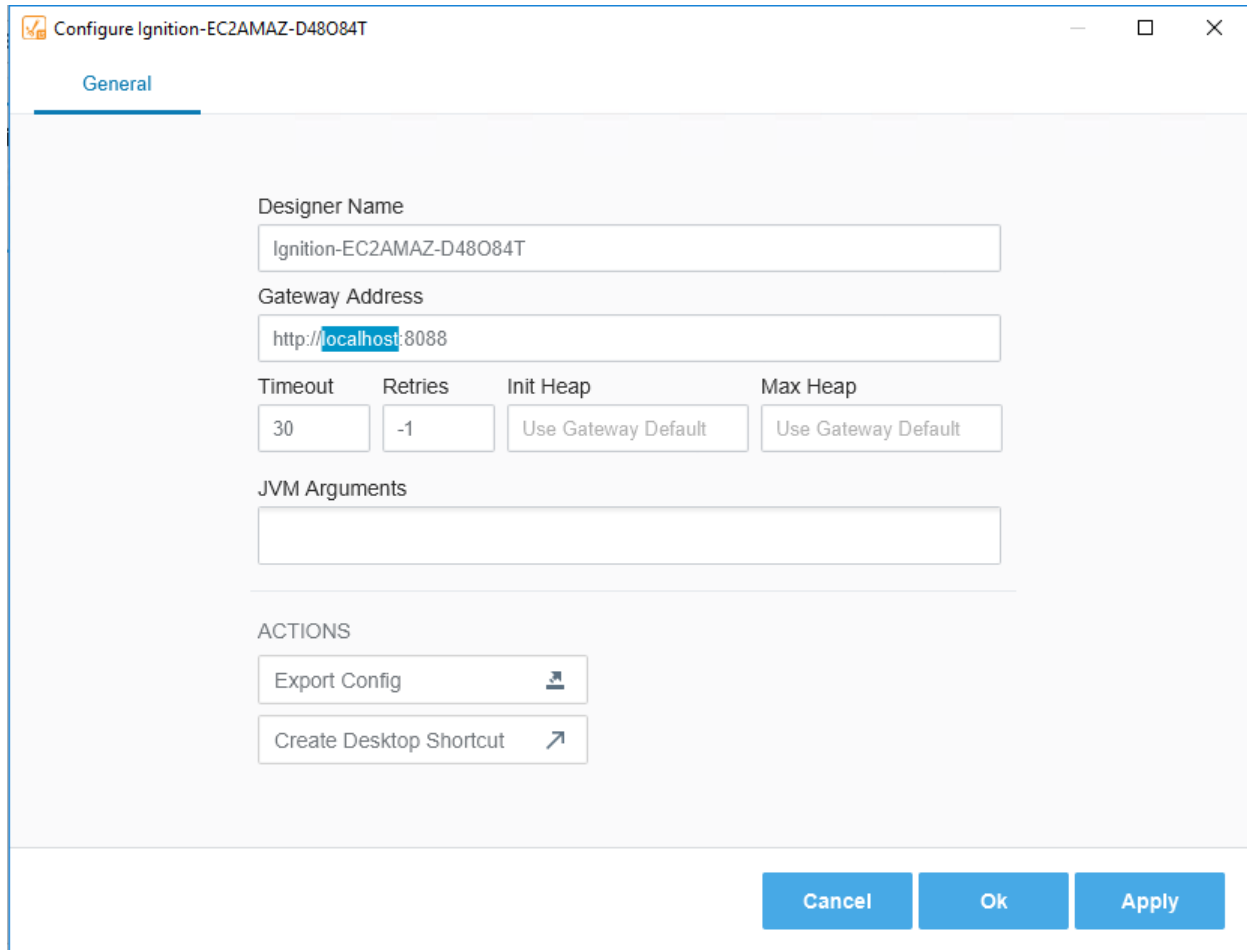
To ensure the Ignition Designer is properly connected, please follow the next steps.



Click the vertical ellipses and then click “Manage” from the prompted window.

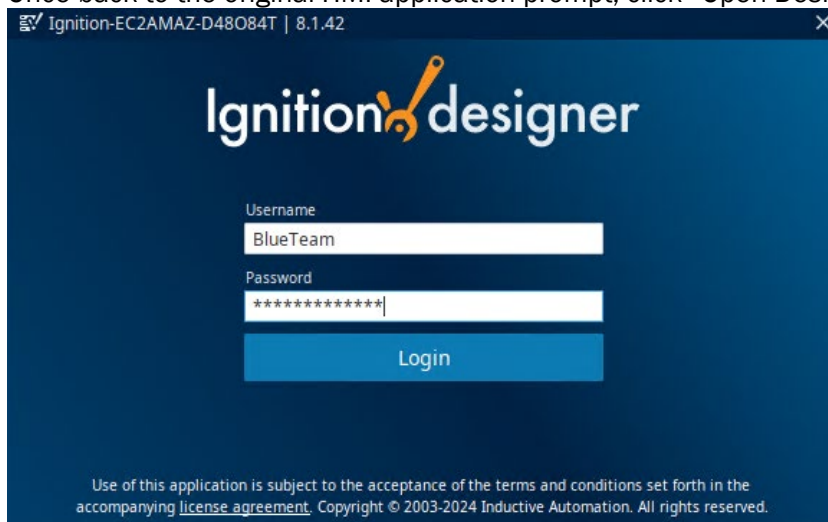


Edit the gateway address to reflect <http://localhost:8080> Click the blue “Apply” button followed by the “Ok” button. Then click the “Open Designer” button to start the designer.



The screenshot shows a configuration window titled "Configure Ignition-EC2AMAZ-D48O84T". The "General" tab is selected. The "Designer Name" field contains "Ignition-EC2AMAZ-D48O84T". The "Gateway Address" field contains "http://localhost:8088". Below these are four fields: "Timeout" (30), "Retries" (-1), "Init Heap" (Use Gateway Default), and "Max Heap" (Use Gateway Default). The "JVM Arguments" field is empty. At the bottom, there are two buttons: "Export Config" and "Create Desktop Shortcut". At the very bottom of the window are three buttons: "Cancel", "Ok", and "Apply".

Once back to the original HMI application prompt, click “Open Designer”.



The screenshot shows the Ignition Designer login screen. The title bar reads "Ignition-EC2AMAZ-D48O84T | 8.1.42". The main area has the "Ignition designer" logo. Below the logo are two input fields: "Username" with the text "BlueTeam" and "Password" with masked characters "*****". A blue "Login" button is below the password field. At the bottom, there is a small line of text: "Use of this application is subject to the acceptance of the terms and conditions set forth in the accompanying [license agreement](#). Copyright © 2003-2024 Inductive Automation. All rights reserved."

Once logged in, please click the “OPEN” button to proceed into the Designer application.

Ignition-EC2AMAZ-D48084T — Open/Create Project

×

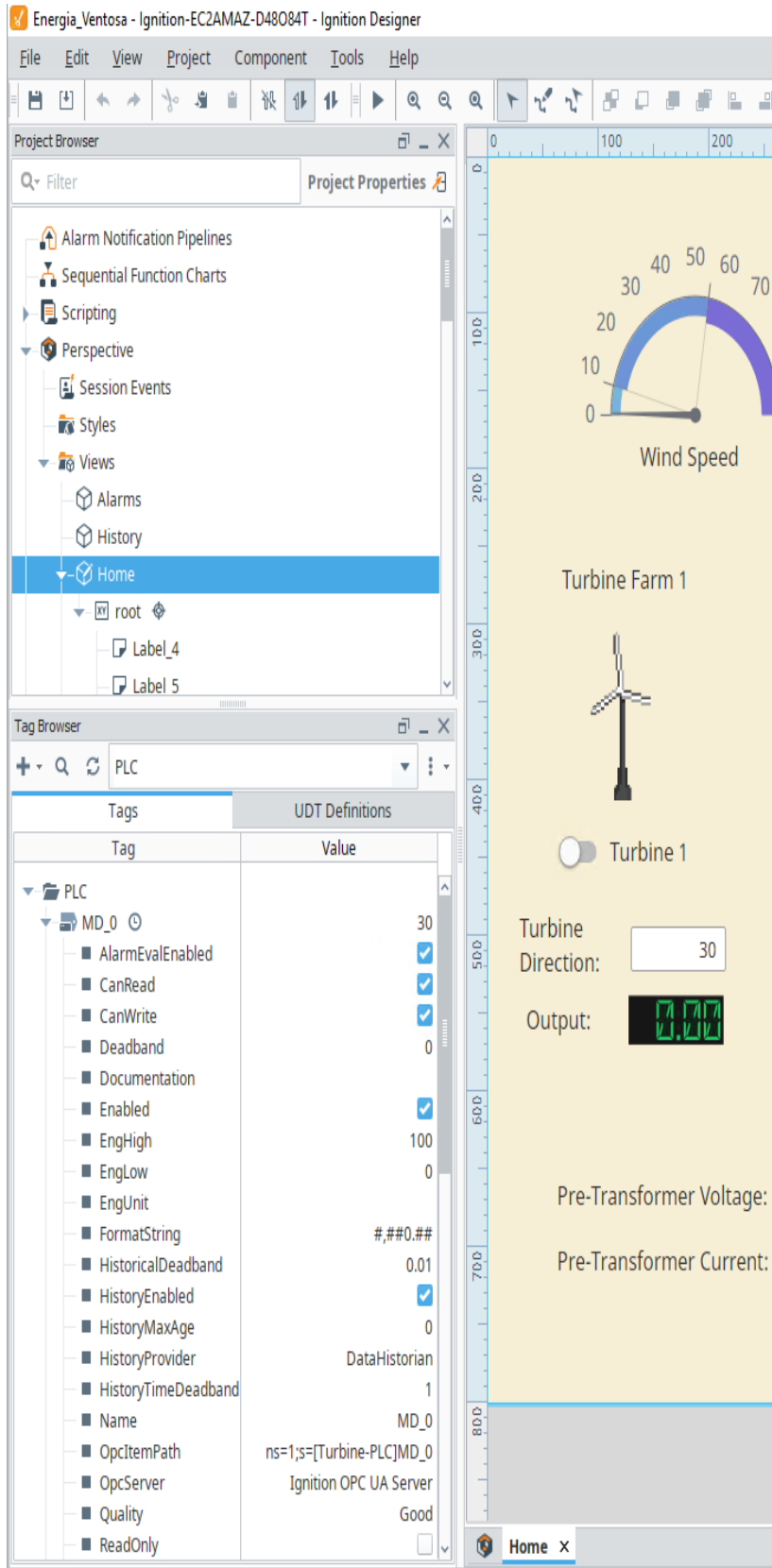
Ignitiondesigner

+ New Project

Filter Projects

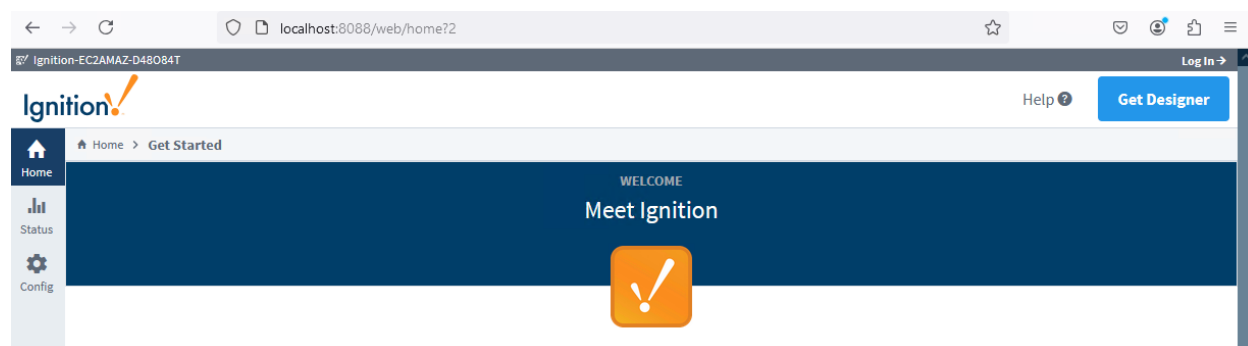
Import Project

Name	Title	Inheritable	Inheritance Hierarchy	Actions
Energia_Ventosa	HMI	false		OPEN

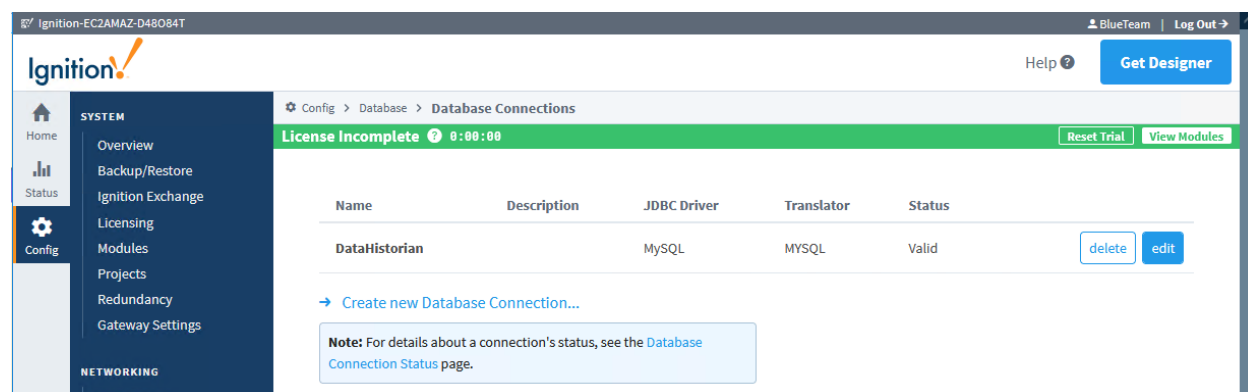


The image at the left shows the Ignition Designer application. Here is where all of the tag and database data can flow into the HMI views to indicate the current status', alarms, modbus data, etc. Each page view is constructed to show the necessary data to be shown to an engineer along with the appropriate switches and a manual override to utilize if necessary. Each tag corresponds to the designated modbus coil or register it is assigned, along with the corresponding database table attributes.

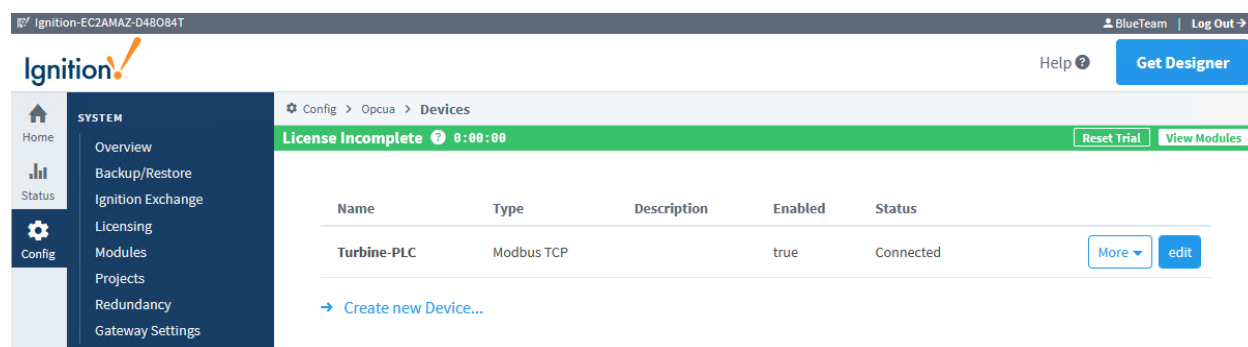
To access the Ignition Gateway, where all of the driver connections are established, browser to localhost:8088 and the Ignition splash page will appear and allow login with **BlueTeam : BlueTeam2024!**



Once logged in, on the left-hand side, there are configuration tabs to drill down further into each type of connection for the HMI. The below image shows the database connection breakdown.



The image below shows the OPCUA connection breakdown for grabbing modbus data from coils and registers.



Upon Initially receiving your CNC virtual machine, you will need to edit the hostname of the PLC in OPC UA connection. To do this, you will click "edit" on "Turbine-PLC" device found on the OPC UA Device connections page and update the Hostname field with the private IP of your PLC virtual machine.

Ignition-EC2AMAZ-D48084T

BlueTeam | Log Out

Ignition

Help

Get Designer

Home

Status

Config

SYSTEM

Overview

Backup/Restore

Ignition Exchange

Licensing

Modules

Projects

Redundancy

Gateway Settings

NETWORKING

Web Server

Email Settings

Gateway Network

SECURITY

General

Auditing

Users, Roles

Service Security

Identity Providers

OAuth2 Clients

Security Levels

Security Zones

DATABASES

Connections

Drivers

Store and Forward

ALARMING

General

Search...

Config > Opcua > Devices

License Incomplete 0:00:00

Reset Trial

View Modules

General

Name

Turbine-PLC

Description

Enabled

☒

(default: true)

Connectivity

Hostname

10.0.52.140

Hostname/IP address of the Modbus device.

Port

502

Port to connect to.

(default: 502)

Local Address

Address of network adapter to connect from.

(default:)

Communication Timeout

2000

Maximum amount of time to wait for a response.

(default: 2,000)

☐ Show advanced properties

Save Changes

The following image is a further drill-down into each OPC quick client connection. This can show each read and write from/to modbus.

Ignition-EC2AMAZ-D48084T

BlueTeam | Log Out

Ignition

Help | Get Designer

Home

Status

Config

SYSTEM

Overview

Backup/Restore

Ignition Exchange

Licensing

Modules

Projects

Redundancy

Gateway Settings

NETWORKING

Web Server

Email Settings

Gateway Network

SECURITY

General

Auditing

Users, Roles

Service Security

Identity Providers

OAuth2 Clients

Security Levels

Security Zones

DATABASES

Connections

Drivers

Store and Forward

Config > Opc > OPC Quick Client

License Incomplete 0:00:00

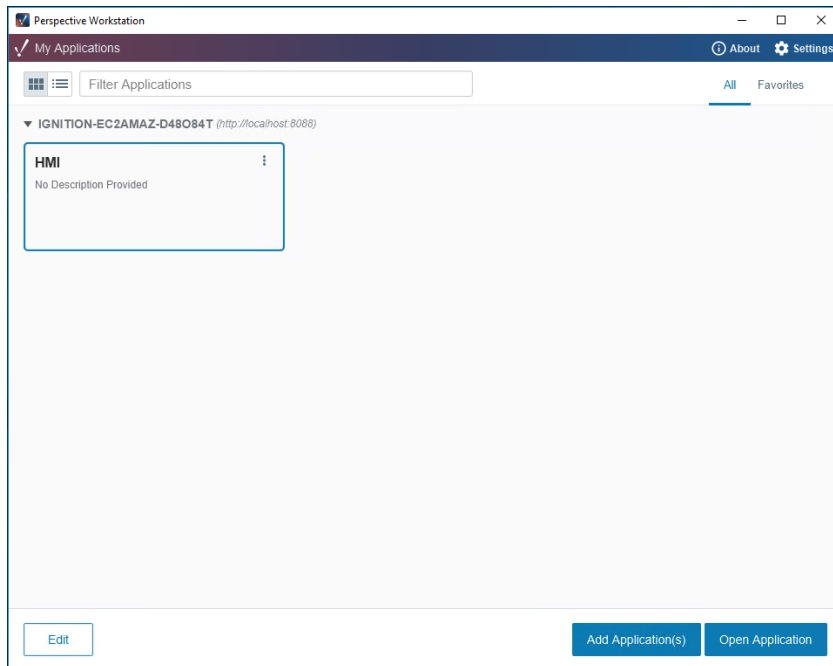
Reset Trial | View Modules

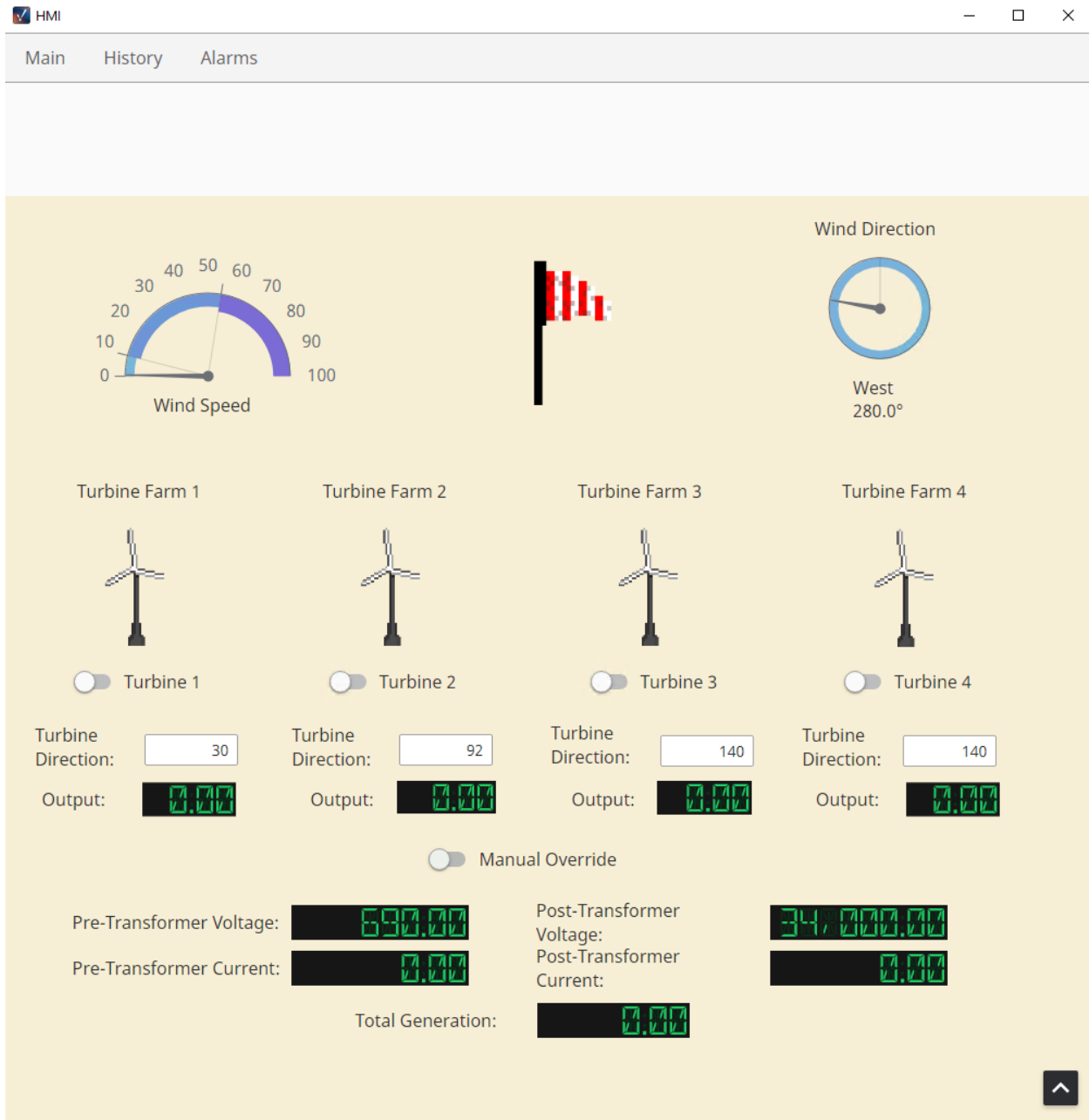
TYPE	ACTION	TITLE
Server	refresh	Ignition OPC UA Server
Object		Devices
Object		[Turbine-PLC]
Object		UnitId 0
Object		MD_0-MD_19
Tag	[s][r][w]	MD_0
Tag	[s][r][w]	MD_1
Tag	[s][r][w]	MD_2
Tag	[s][r][w]	MD_3
Tag	[s][r][w]	MD_4
Tag	[s][r][w]	MD_5
Tag	[s][r][w]	MD_6
Tag	[s][r][w]	MD_7
Tag	[s][r][w]	MD_8

Subscription 1 [x] [Add]

Server	Address	Value	Quality	Timestamp
Subscription name : Rate (ms) : Set				
Subscription 1		1000		

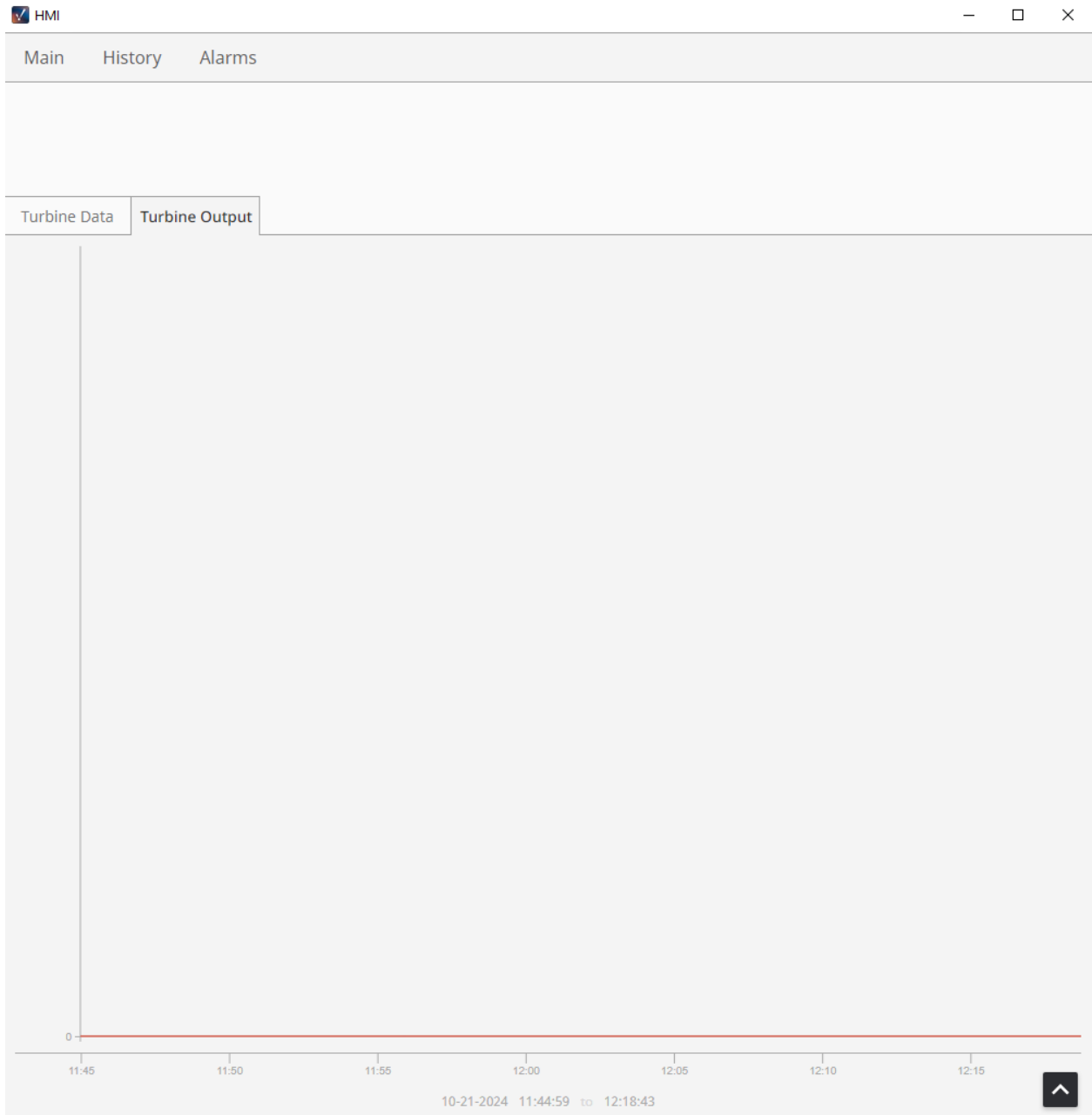
To start the Perspective Engineering Workstation view, click on the desktop icon to bring up the Perspective Workstation application. Click on the HMI application within and click the “Open Application” button. You will be prompted for login credentials.





The main page of the HMI will appear. This is where you can engage with the manual_override and turbine coils directly, along with the turbine direction registers.

The History page directly corresponds to the data historian passed between both the HMI and the database in both table and graph form.



HMI

Main

History

Alarms

6 ACTIVE

0 SHELVED

Active, Unacknowledged

Active, Acknowledged

Cleared, Unacknowledged

Priority: Low

Priority: Medium

Priority: High

Priority: Critical

Remove All

Active Time	Display Path	Priority	State	Source	Name
10/21/2024 11:44:59	PLC/QX_4/ManualOverride	Critical	Active, Unac...	prov:PLC:/tag:PLC/QX_4:/alm...	ManualOver...
10/21/2024 11:44:59	PLC/QX_0/Turbine Off	Low	Active, Unac...	prov:PLC:/tag:PLC/QX_0:/alm...	Turbine Off
10/21/2024 11:44:59	PLC/QX_3/Turbine Off	Low	Active, Unac...	prov:PLC:/tag:PLC/QX_3:/alm...	Turbine Off
10/21/2024 11:44:59	PLC/MD_18/Wind Speed LOW	Low	Active, Unac...	prov:PLC:/tag:PLC/MD_18:/al...	Wind Speed ...
10/21/2024 11:44:59	PLC/QX_2/Turbine Off	Low	Active, Unac...	prov:PLC:/tag:PLC/QX_2:/alm...	Turbine Off
10/21/2024 11:44:59	PLC/QX_1/Turbine Off	Low	Active, Unac...	prov:PLC:/tag:PLC/QX_1:/alm...	Turbine Off

25 rows

1

6 alarm events

Last 8 hours

Priority: Low

Priority: Medium

Priority: High

Priority: Critical

Remove All

Event Time	Event Id	Source	Event State	Priority
10/21/2024 11:44:59	c362a557-0b91-481f-af53-7f2d5415e015	prov:PLC:/tag:PLC/QX_4:/al...	Active	Critical
10/21/2024 11:44:59	51725129-f956-4266-8860-289debfa1a27	prov:PLC:/tag:PLC/QX_0:/al...	Active	Low
10/21/2024 11:44:59	927244c5-10d6-4466-bb57-d175ca94b6...	prov:PLC:/tag:PLC/QX_1:/al...	Active	Low
10/21/2024 11:45:00	3c997861-d03b-4307-b8b5-979154cc54...	prov:PLC:/tag:PLC/QX_2:/al...	Active	Low
10/21/2024 11:45:00	315b769a-d8ba-4459-ac32-f14de08078...	prov:PLC:/tag:PLC/MD_18:/a...	Active	Low
10/21/2024 11:45:00	a8a71e56-1c2c-41a8-82e9-cb4e10f9d1c0	prov:PLC:/tag:PLC/QX_3:/al...	Active	Low

25 rows

1

6 alarm events

Last 8 hours

Priority: Low

Priority: Medium

Priority: High

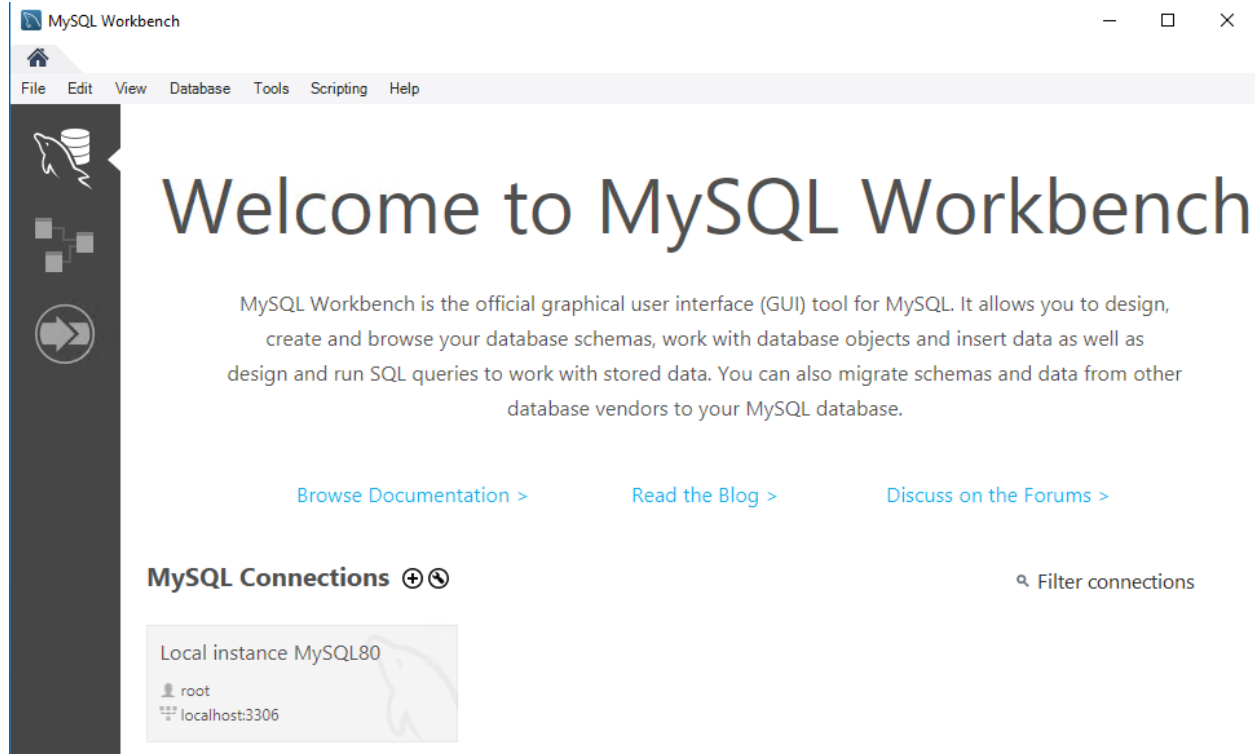
Priority: Critical

Remove All

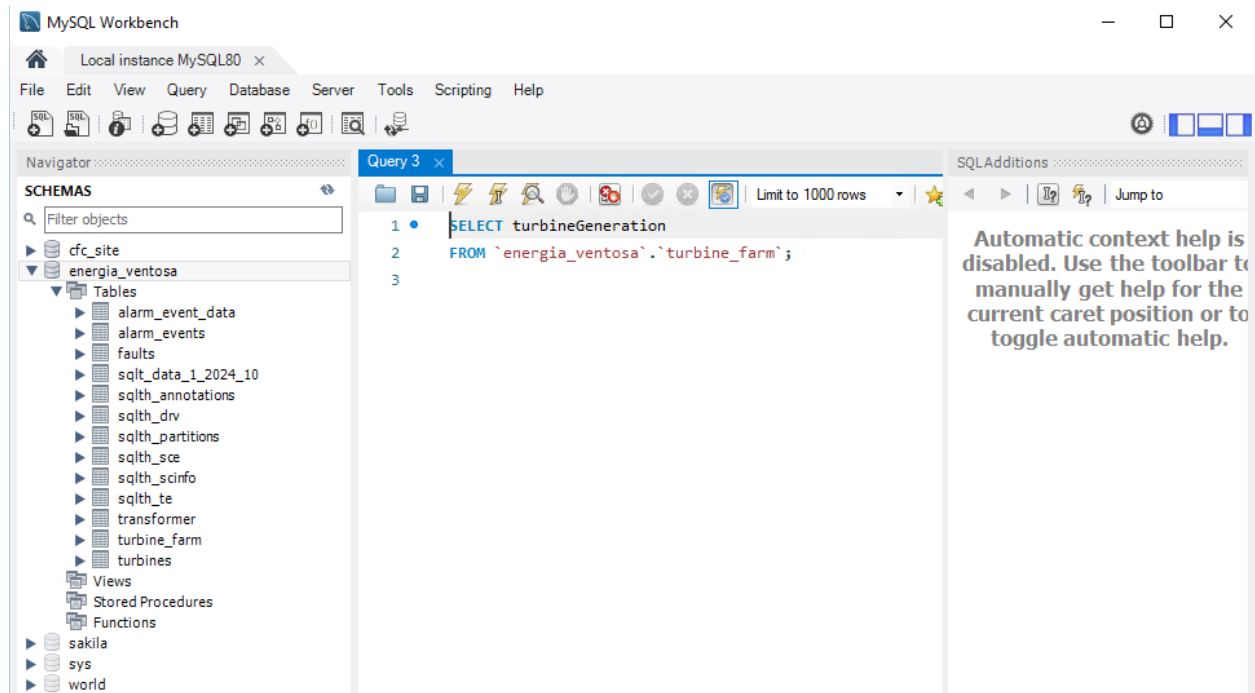
The Alarms page shows all of the system alarms and provides the user the ability to acknowledge, shelf, or remove all alarms thrown by system threshold logic.

Below is an image of MySQL Workbench which is installed on the workstation for ease of access, or the terminal works as well for the data historian database.

The credentials are **root : thisismypassword** and should not be changed.



Below you can see the energia_ventosa database table structure breakdown.



ENERGIA VENTOSA ENERGY GRID MAP

Within your AWS EC2 dashboard, you will see a VM named, “MapBox (**Do Not Touch**)”. This is your team’s visual mapping system for the competition. You should make sure this VM is turned on and running the day before the competition. You will start it like all your others and then following the steps below, attempt to ensure you can connect to it.

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
<input type="checkbox"/>	Public Database	i-0b1a690bc29b9c0d1	Stopped	t3.medium	–	View alarms	us-east-2a
<input type="checkbox"/>	Task	i-0d0a28e6b8ffde14d	Stopped	t3.medium	–	View alarms	us-east-2a
<input type="checkbox"/>	CNC	i-08704e46c921478e6	Running	t3.medium	3/3 checks passed	View alarms	us-east-2a
<input checked="" type="checkbox"/>	MapBox (Do Not Touch)	i-022e2e7b81a22234c	Running	t3.medium	3/3 checks passed	View alarms	us-east-2a
<input type="checkbox"/>	PLC	i-005abe5918c63b445	Running	t3.medium	3/3 checks passed	View alarms	us-east-2a
<input type="checkbox"/>	AD	i-0c6a266c259e0a125	Stopped	t3.medium	–	View alarms	us-east-2a
<input type="checkbox"/>	Web Server	i-00f8c99b90092ce2d	Stopped	t3.medium	–	View alarms	us-east-2a

After the VM has been started, you can click on the Instance ID and it will prompt a more informative page about that VM. On the top right you will find the Private IPv4 Address. You will utilize this within a browser to establish your connect to the WebGL map.

[EC2](#) > [Instances](#) > i-022e2e7b81a22234c

Instance summary for i-022e2e7b81a22234c (MapBox (Do Not Touch)) [Info](#)

[Connect](#) [Instance state](#)

[Actions](#)

Instance ID

i-022e2e7b81a22234c (MapBox (Do Not Touch))

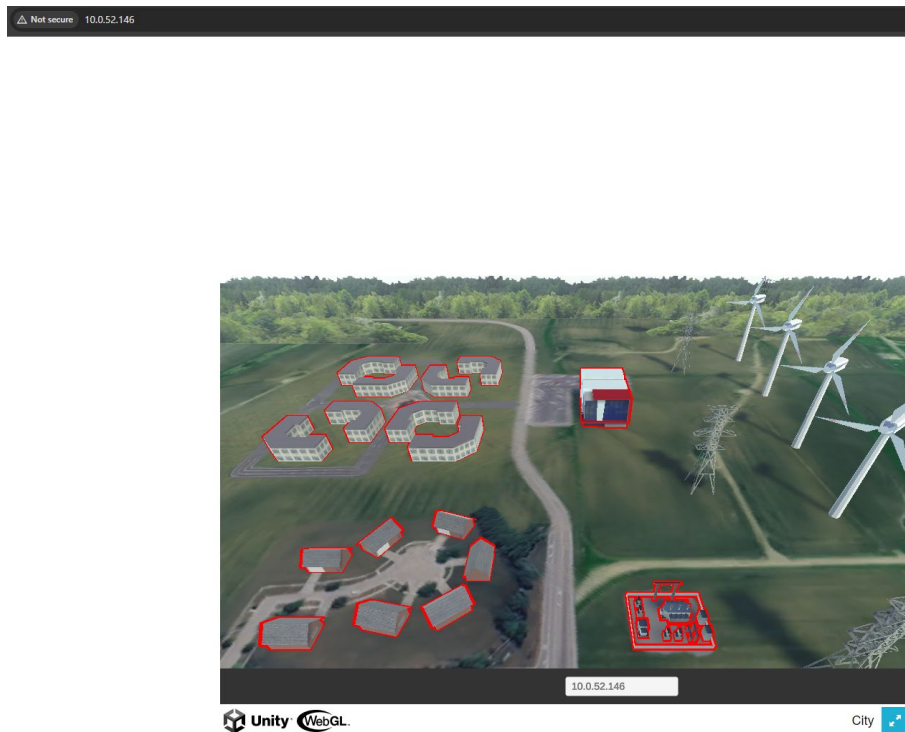
Public IPv4 address

–

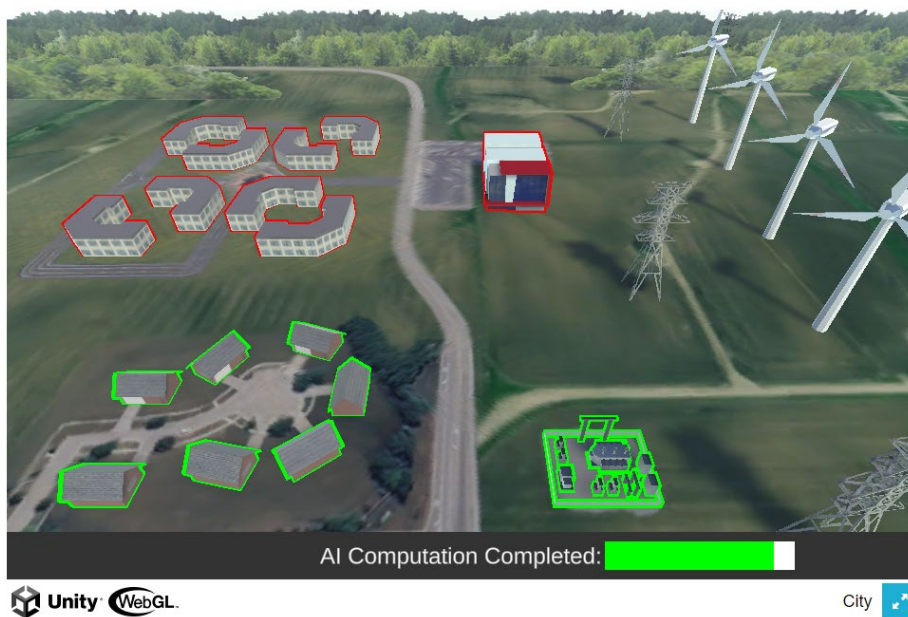
Private IPv4 addresses

10.0.52.146

Here you will take that same IP Address and input it into the text box below the map and hit enter.



Note that until the start of the game, you will likely be seeing no changes and movement to the mapping system, but you should not see the bottom text box change to a bar section that reads, “AI Computation Completed”.



AI Computation Solution Generation Scoring

There are multiple factors to the overall scoring of the AI Computation Solution Generation. The goal of your team is to complete the AI Computation Solution by the end of the competition to earn the maximum number of points.

*** Pre-Competition Flags**

Your team will have the ability to find a total of 7 pre-competition flags within your traditional infrastructure VMs. These flags can be found while discovering and patching/fixing vulnerabilities in the traditional VMs. Once a flag is obtained, your team should input it into the scoreboard to obtain bonus AI computation solution generation. All pre-competition flags need to be submitted prior to the start of the competition.

*** Assume Breach Flags**

When completing assume breach plays, you will receive a flag for each play to input into your team's scoreboard for that specific assume breach play. For each 100% completion of an assumed breach play, you will obtain bonus AI computation solution generation. Flags may be submitted into the scoreboard up until the end of the competition.

*** Data Center Uptime**

It is the responsibility of each team to attempt to generate as much power as possible throughout the competition timeframe as to establish as much grid uptime as can be obtained. Due to the company's system breaches and the automated turbine direction systems taken offline, your team must utilize the HMI to track the wind direction and appropriately adjust the turbine direction in the attempt to generate the most efficient amount of power. By generating enough power, the grid can power the data center, thus resulting in the AI being able to complete computation solution generation. The data center does have a battery backup system but will deplete fast if not charged.

TROUBLESHOOTING COMMON ISSUES

If you notice your Map application is not showing the correct asset status, within AWS, "Reboot Instance" of the MapBox VM.