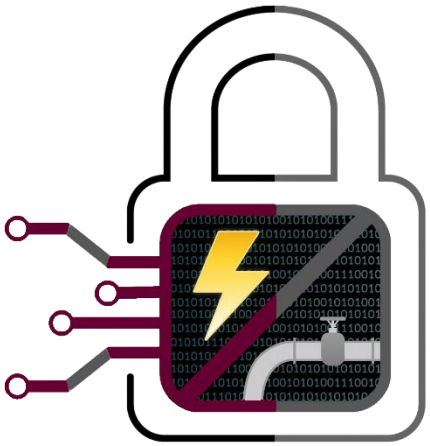


U.S. DEPARTMENT OF ENERGY'S

CYBERFORCE COMPETITION®

DEFENDING U.S. ENERGY INFRASTRUCTURE

ICS Documentation

2025

CYBERFORCE COMPETITION®

CONTENTS

NOTE

Both the HMI/CNC and PLC VMs are within the Assume Breach Infrastructure and **EXTREME CAUTION** should be used when attempting to alter these machines.

CONNECTIVITY

PLC

Ubuntu 22.04

plc.<bluexxxx>.cfc.local

blueteam : BlueTeam2025!

PLC - :502

CNC/HMI

Windows Server 2019

cnc.<bluexxxx>.cfc.local

blueteam : BlueTeam2025!

Ignition Gateway - :8088

blueteam : BlueTeam2025!

Data Historian MySQL - 3306

blueteam : BlueTeam2025!

For more information about Ignition please visit:
https://www.inductiveuniversity.com/courses/ignition/ignition-overview/8.1

OBSIDIAN PEARL INDUSTRIAL CONTROL SYSTEM MANUAL

REGISTERS (2048-2114) AND COILS (0000-0022)

```
SafeToOperate AT %QX0.0 : BOOL := FALSE;
StartSystem AT %QX0.1 : BOOL := FALSE;
StopSystem AT %QX0.2 : BOOL := FALSE;
FireDetected AT %QX0.3 : BOOL := FALSE;
ESDActive AT %QX0.4 : BOOL := FALSE;
ManualOverride AT %QX0.5 : BOOL := FALSE;
CheckFlarePilot AT %QX0.7 : BOOL := FALSE;
FlareRequired AT %QX0.8 : BOOL := FALSE;
FireSuppressionPump AT %QX0.9 : BOOL := FALSE;
BOP AT %QX0.10 : BOOL := FALSE;
FlareIgniter AT %QX0.11 : BOOL := FALSE;
SystemStartLatch AT %QX0.12 : BOOL := FALSE;
WellValve AT %QX0.13 : BOOL := FALSE;
```

```
Separator AT %QX0.14 : BOOL := FALSE;
InletFlowActive AT %QX0.15 : BOOL := FALSE;
OilDumpValve AT %QX0.16 : BOOL := FALSE;
WaterDumpValve AT %QX0.17 : BOOL := FALSE;
GasOutletValve AT %QX0.18 : BOOL := FALSE;
FlareValve AT %QX0.19 : BOOL := FALSE;
WaterInjectPump AT %QX0.20 : BOOL := FALSE;
ExportPump AT %QX0.21 : BOOL := FALSE;
FlowAlert AT %QX0.22 : BOOL := FALSE;

WellPressure AT %MD0 : REAL := 0.0;
WellTemp AT %MD1 : REAL := 0.0;
WellFlowRate AT %MD2 : REAL := 0.0;
MaxWellPressure AT %MD3 : REAL := 5000.0;
MaxWellTemp AT %MD4 : REAL := 95.0;
MinWellFlowRate AT %MD5 : REAL := 0.17;
MaxWellFlowRate AT %MD6 : REAL := 10.42;
SeparatorTemp AT %MD7 : REAL := 0.0;
SepOilLevel AT %MD8 : REAL := 0.0;
SepWaterLevel AT %MD9 : REAL := 0.0;
SepGasLevel AT %MD10 : REAL := 0.0;
WaterOut AT %MD11 : REAL := 0.0;
GasOut AT %MD12 : REAL := 0.0;
OilOut AT %MD13 : REAL := 0.0;
SepMaxTemp AT %MD14 : REAL := 90.0;
SepMinTemp AT %MD15 : REAL := 20.0;
MaxOilLevel AT %MD16 : REAL := 80.0;
MinOilLevel AT %MD17 : REAL := 4.9;
MaxWaterLevel AT %MD18 : REAL := 80.0;
MinWaterLevel AT %MD19 : REAL := 2.1;
MaxGasLevel AT %MD20 : REAL := 72000.0;
MinGasLevel AT %MD21 : REAL := 5600.0;
ExportPressure AT %MD22 : REAL := 0.0;
ExportPumpVibration AT %MD23 : REAL := 0.0;
ExportPumpTemp AT %MD24 : REAL := 0.0;
MaxExportPumpTemp AT %MD25 : REAL := 95.0;
MaxExportPressure AT %MD26 : REAL := 500.0;
MaxExportPumpVibration AT %MD27 : REAL := 5.0;
MinExportFlow AT %MD28 : REAL := 10.0;
MaxExportFlow AT %MD29 : REAL := 40.0;
FlowIn AT %MD30 : REAL := 0.0;
FlowOut AT %MD31 : REAL := 0.0;
FlowTolerance AT %MD32 : REAL := 1.0;
Weather AT %MD33 : REAL := 1.0;
```

SYSTEM ALERTS AND THRESHOLDS

If the WellPressure is above 5000.0, Blowout Prevention is Enabled.

If the WellTemp is above 95.0, Blowout Prevention is Enabled.

If FireDetected or a Hurricane is Detected, SafeToOperate is Disabled.

If SafeTooOperate is Disabled, Emergency Shutdown procedures start.

If the WellFlowRate is less than 10.42 and greater than 0.17 Oil generation will begin.

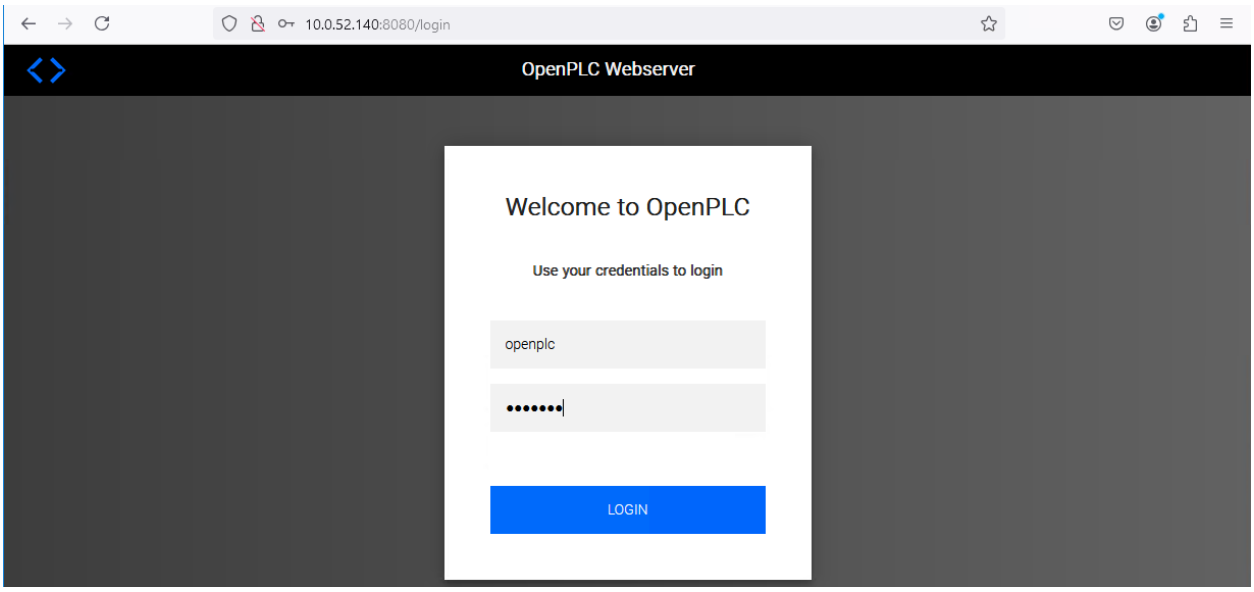
If SeparatorTemp is less than 90.0 and greater than 20.0 The Separator will enable.

If ExportPumpVibration is less than 5.0 and ExportPumpTemp is less than 95.0 and ExportPressure is less than 500.0

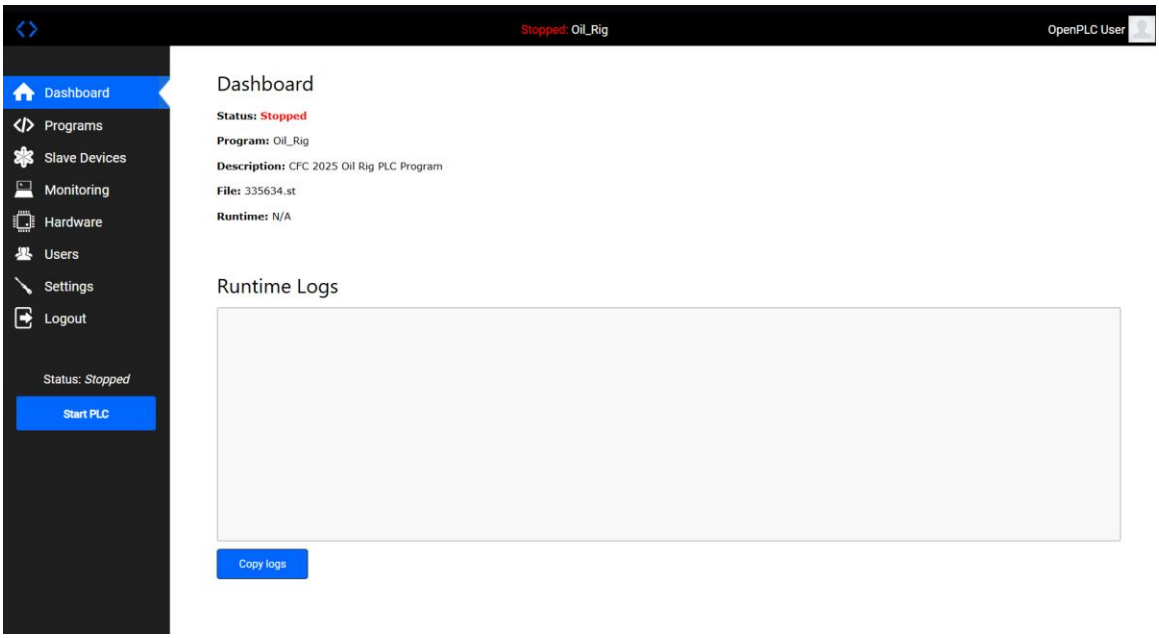
OilOut is calculated based on WellFlowRate.

PLC

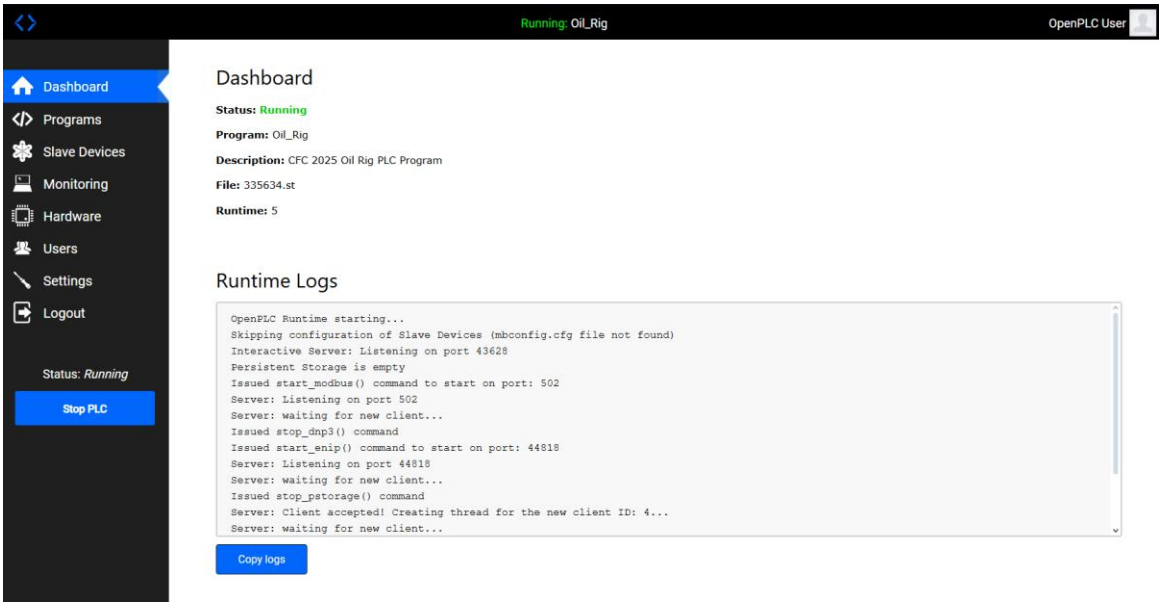
First, we must begin by starting the PLC, by going to <plc-ip>:8080. Here you will see the OpenPLC web page prompt. The credentials are openplc : openplc



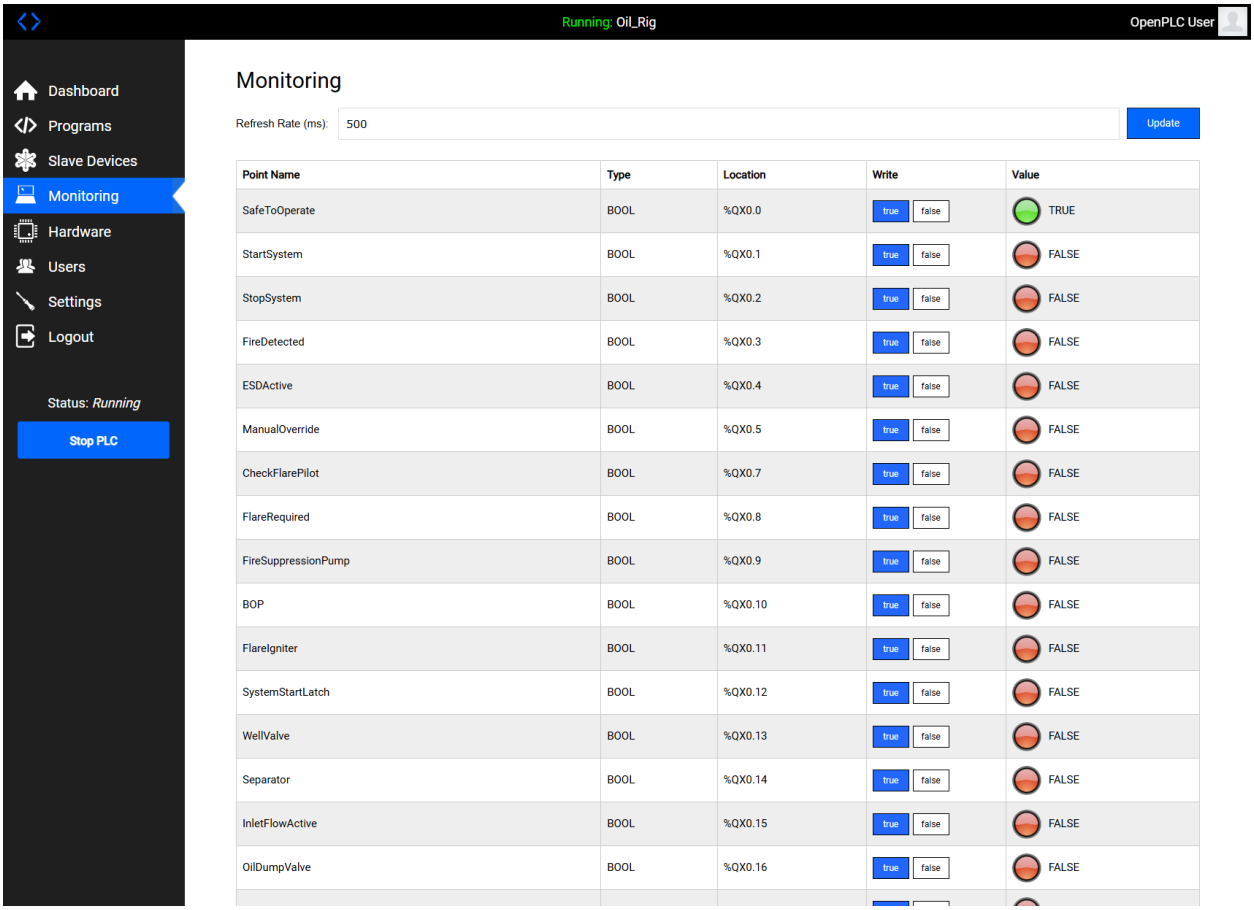
Once logged in you should see the dashboard, from here you can slick the blue button “Start PLC”. This will initialize the Oil_Rig PLC Program.



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



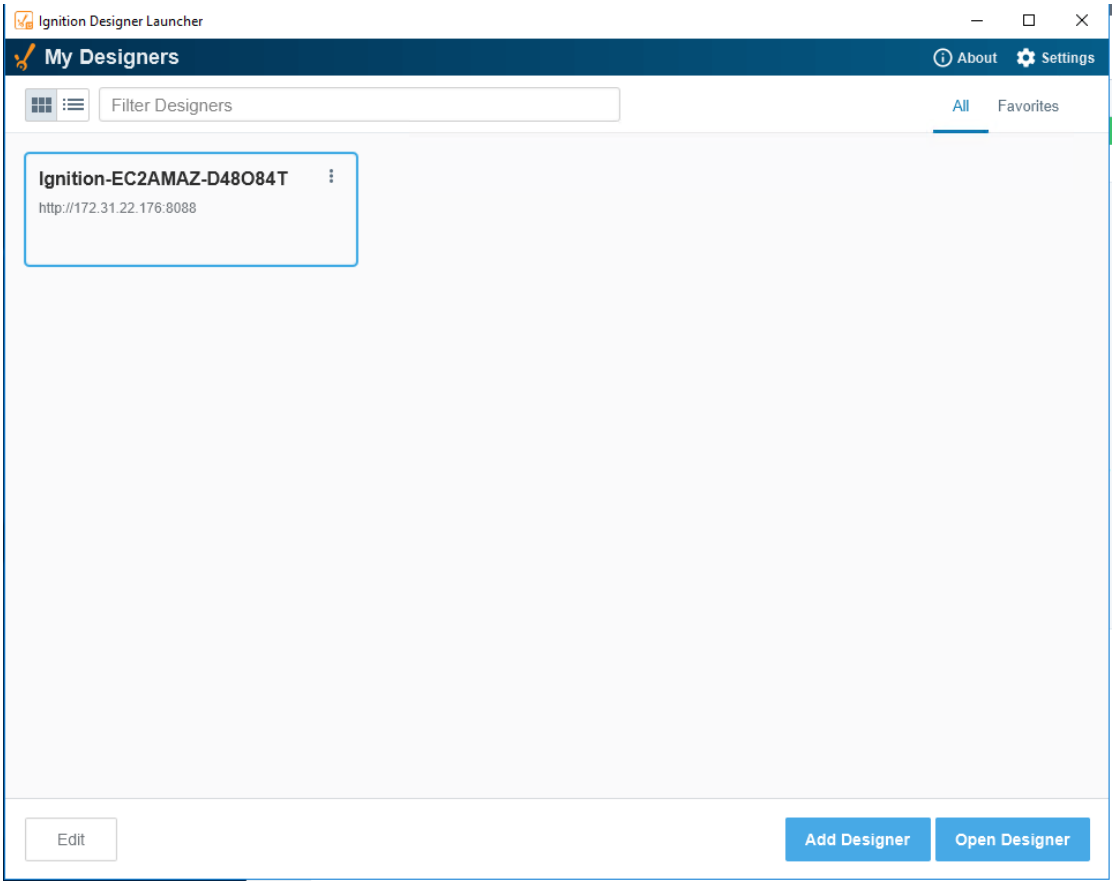
Below is the monitoring display where you can see all the coils and registers associated with the PLC program along with their locations and current values.



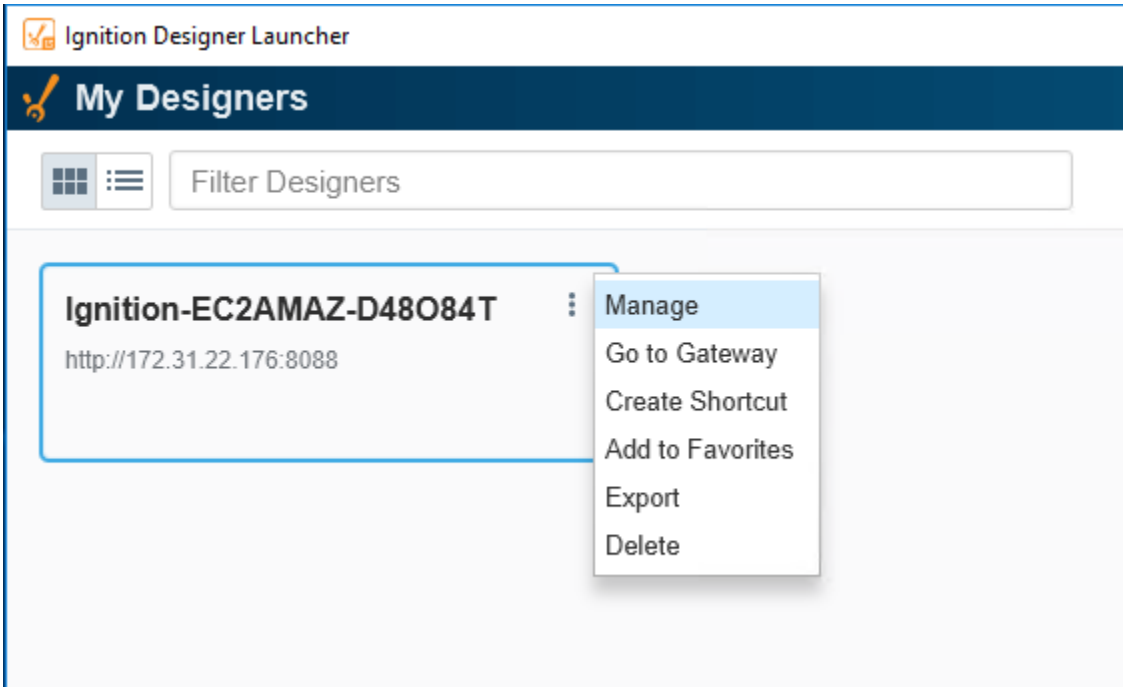
HMI

On the Desktop of the Windows 2019 CnC there are two icons designated for the Ignition HMI. Designer Launcher icon launches the Ignition Designer application, and the Perspective Workstation icon launches the HMI Perspective engineering workstation viewer.

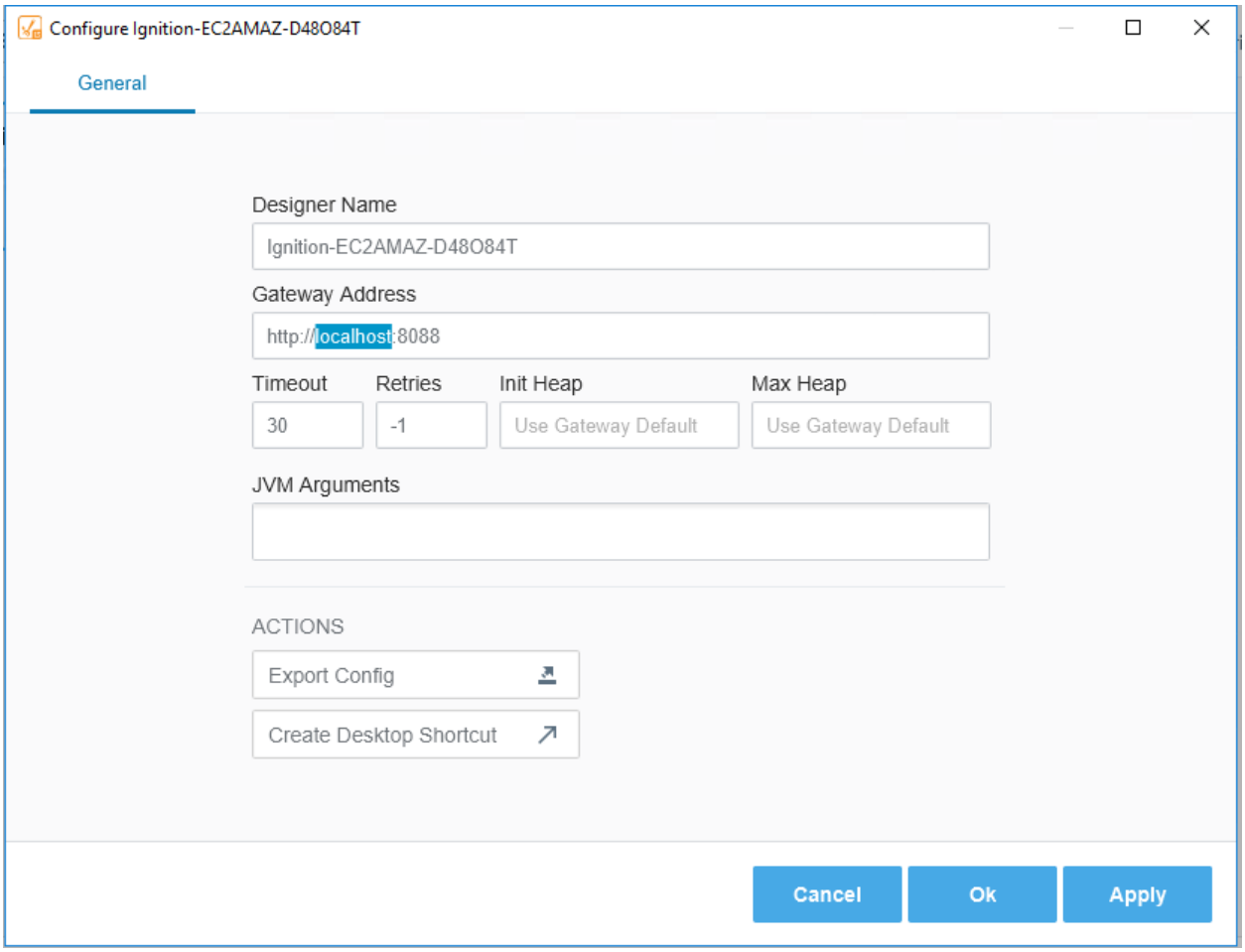
To ensure the Ignition Designer is properly connected, please follow the next steps.

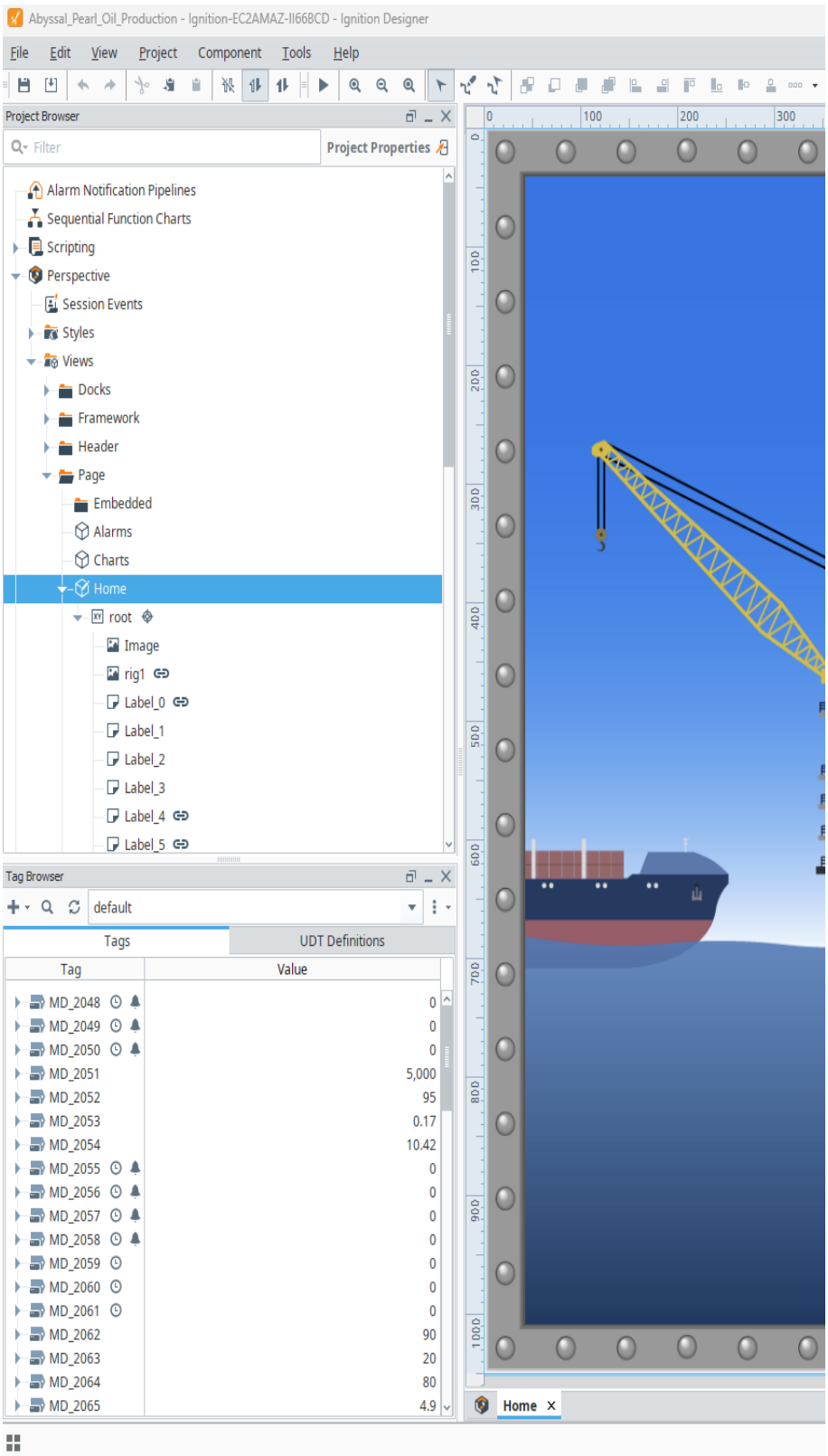


Click the vertical ellipses and then click “Manage” from the prompted window.



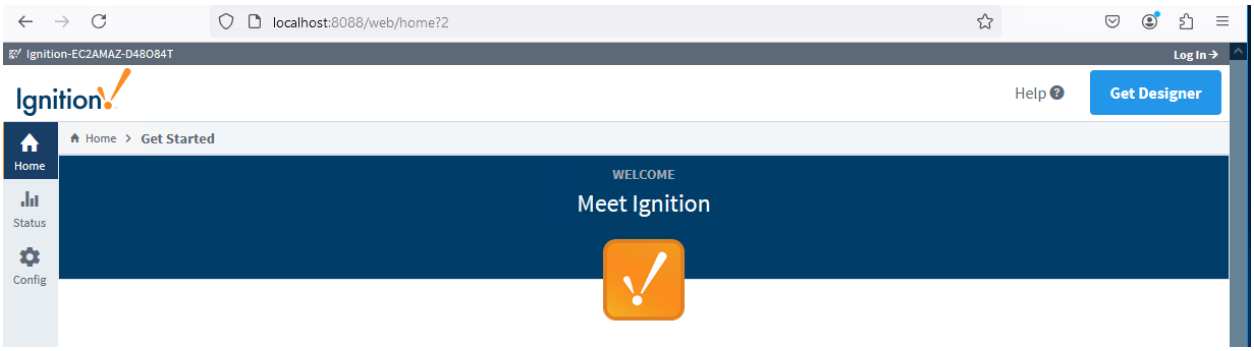
Edit the gateway address to reflect http://localhost:8088 Click the blue “Apply” button followed by the “Ok” button. Then click the “Open Designer” button to start the designer.



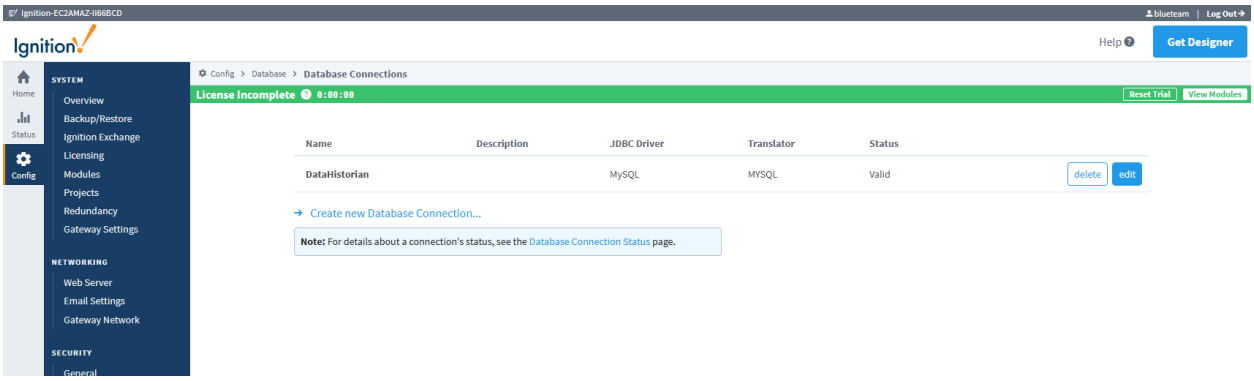


The image on the left shows the Ignition Designer application. Here is where all the tag and database data can flow into the HMI views to indicate the 'current status', alarms, modbus data, etc. Each page view is constructed to show the necessary data to be shown to an engineer along with the appropriate 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.

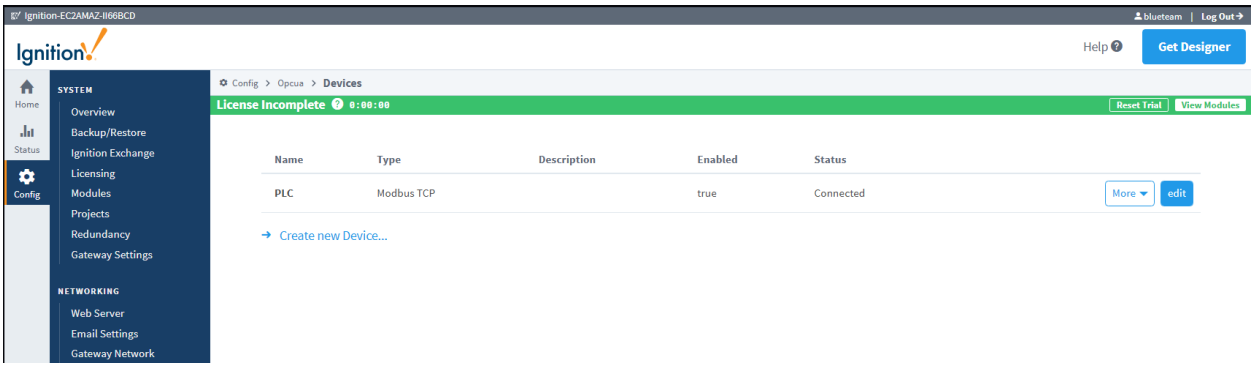
To access the Ignition Gateway, where all the driver connections are established, browser to localhost:8088 and the Ignition splash page will appear and allow login with blueteam: BlueTeam2025!



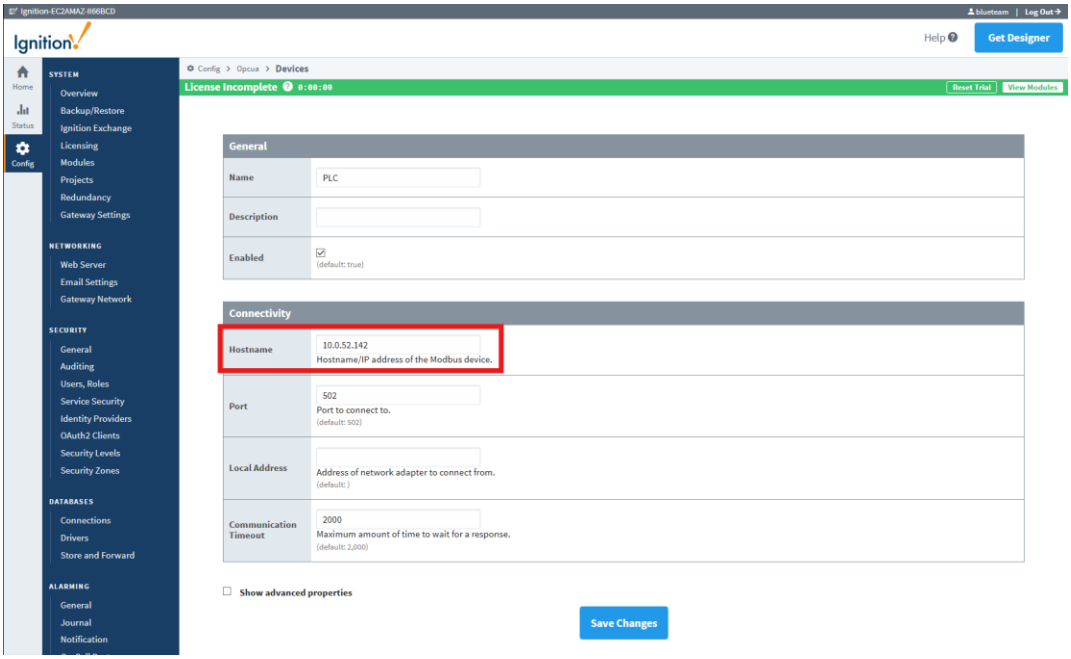
Once logged in, on the left-hand side, there are configuration tabs to drill down further into each type of connection for the HMI. The below image shows the database connection breakdown.



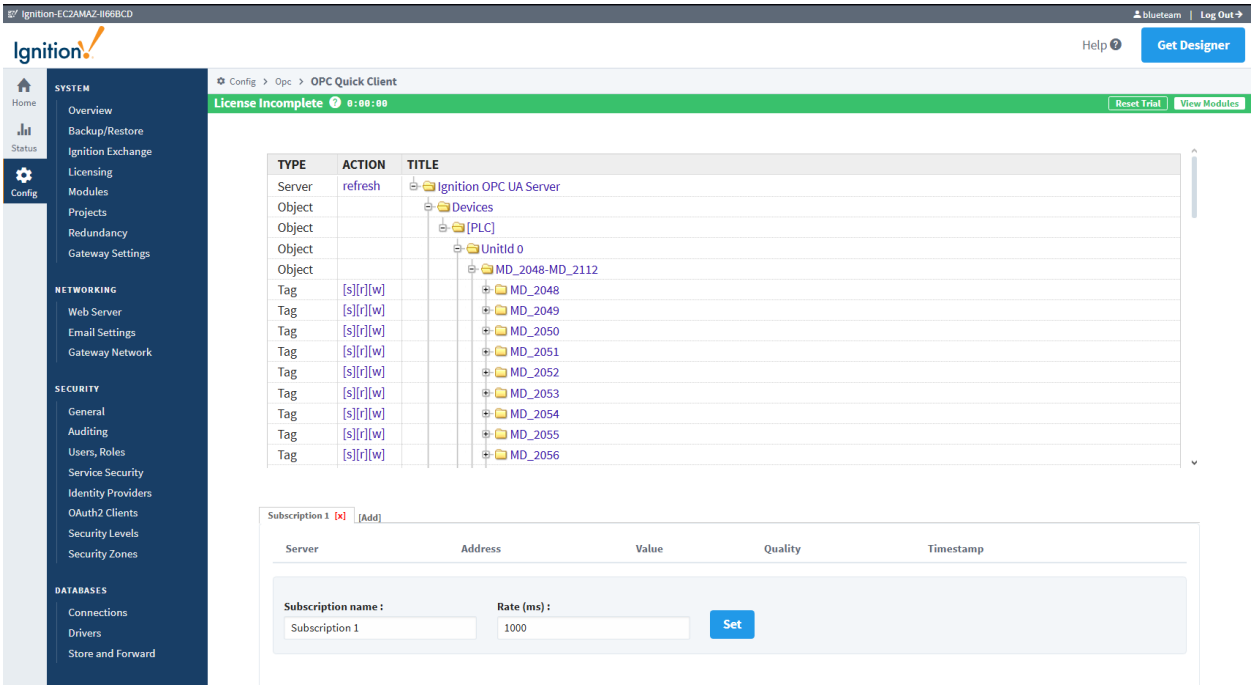
The image below shows the OPCUA connection breakdown for grabbing modbus data from coils and registers.



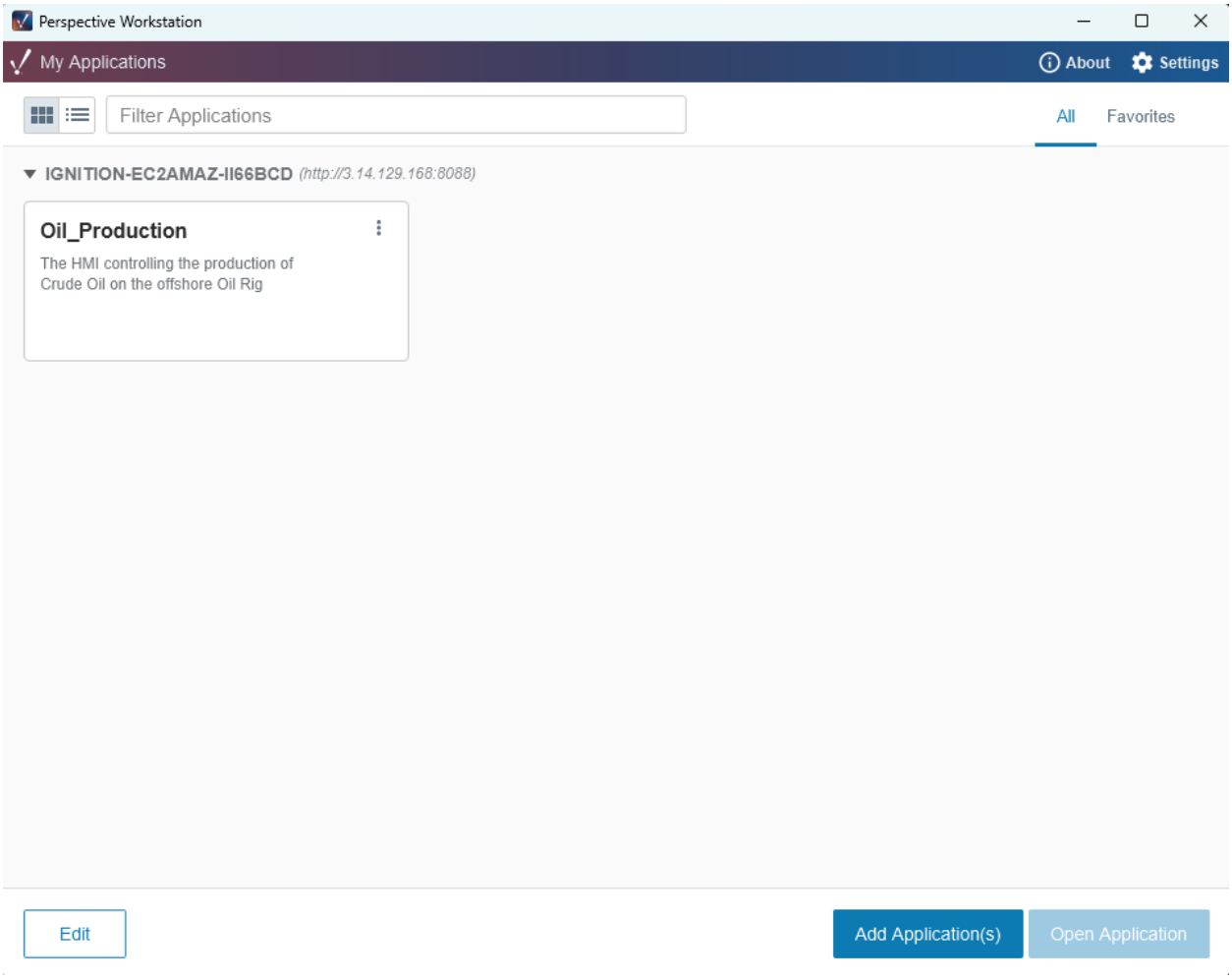
Upon Initially receiving your CNC virtual machine, you will need to edit the hostname of the PLC in OPC UA connection. To do this, you will click "edit" on “PLC” device found on the OPC UA Device connections page and update the Hostname field with the private IP of your PLC virtual machine.

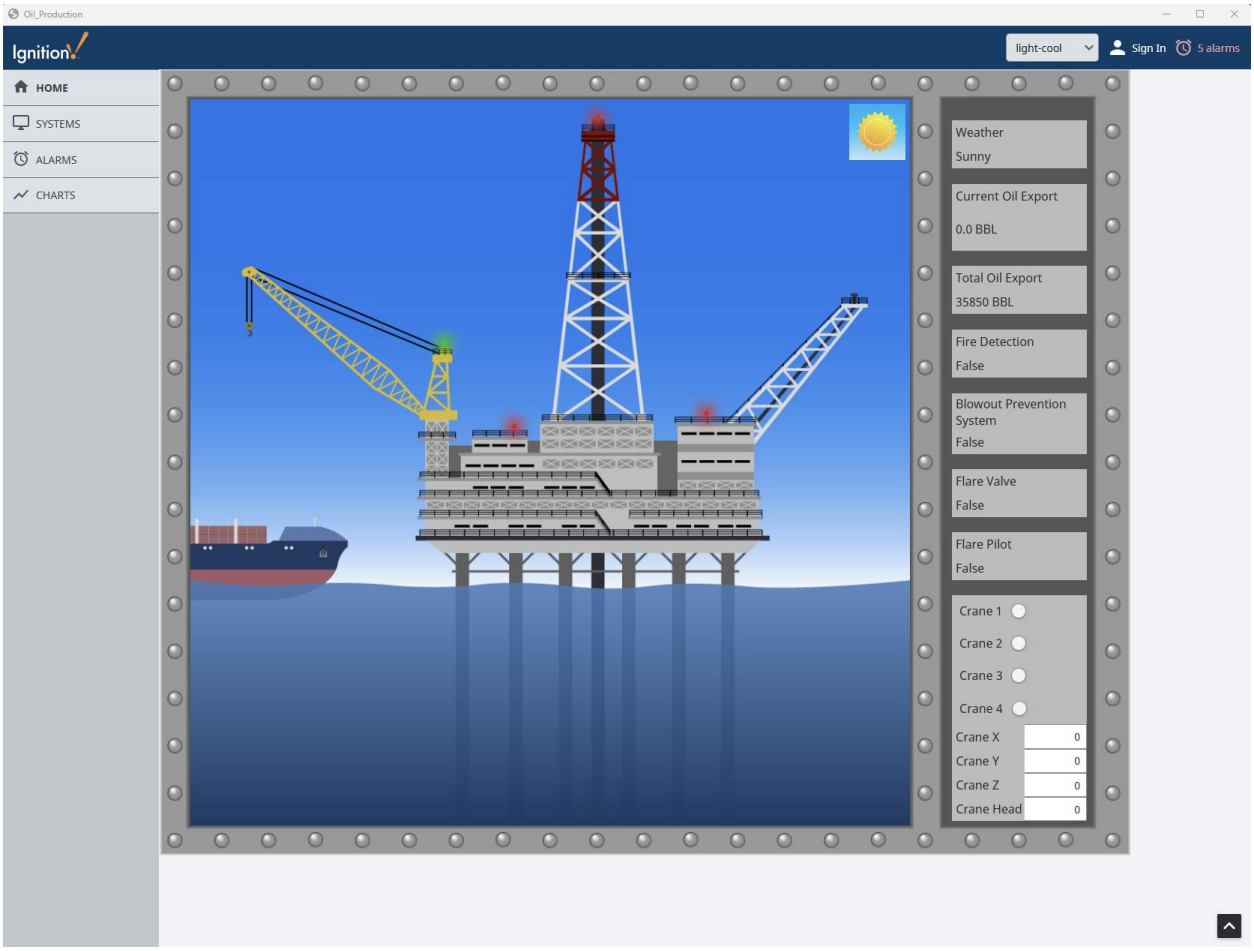


The following image is a further drill-down into each OPC quick client connection. This can show each read and write from/to modbus.

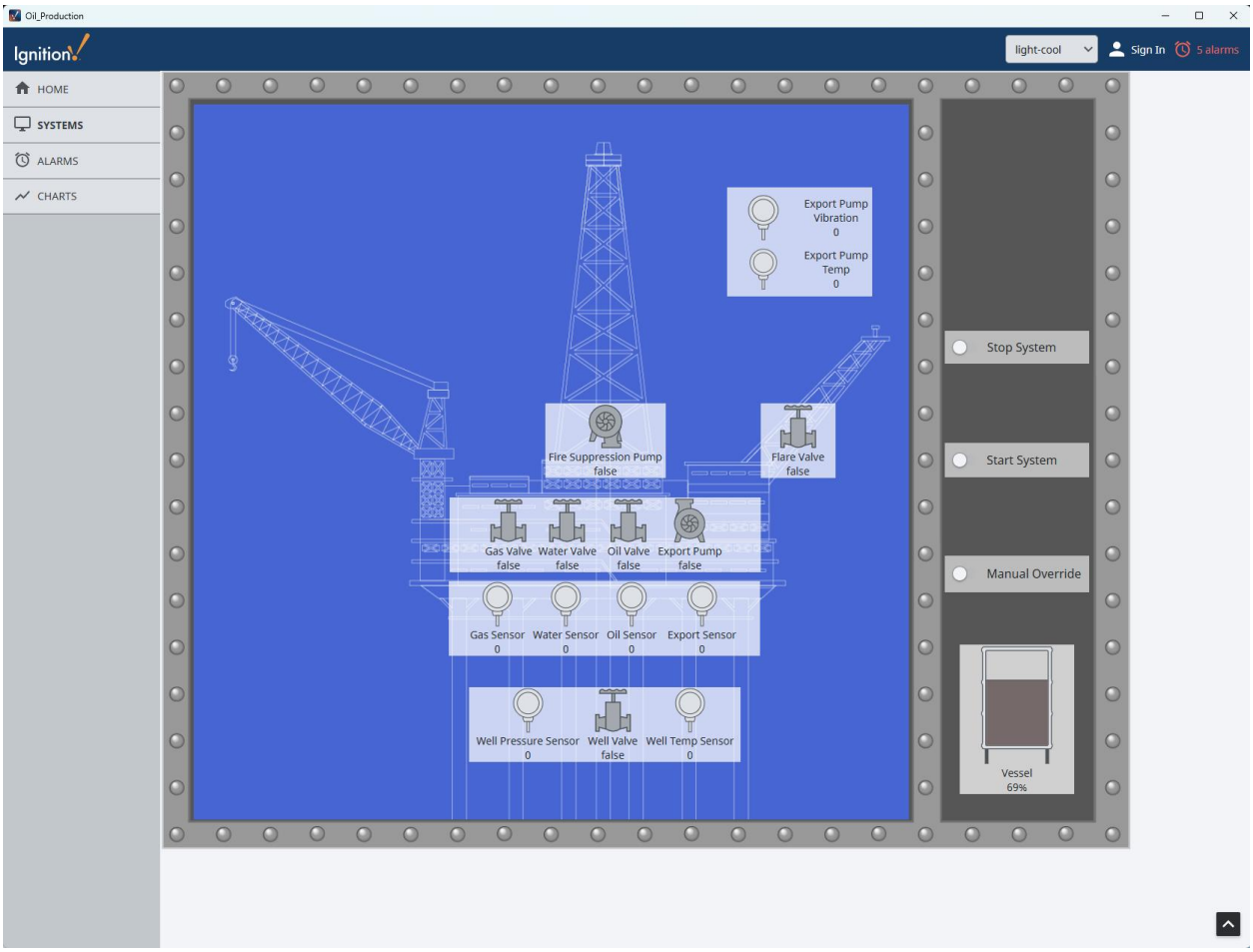


To start the Perspective Engineering Workstation view, click on the desktop icon to bring up the Perspective Workstation application. Click on the HMI application within and click the “Open Application” button. You will be prompted for login credentials.

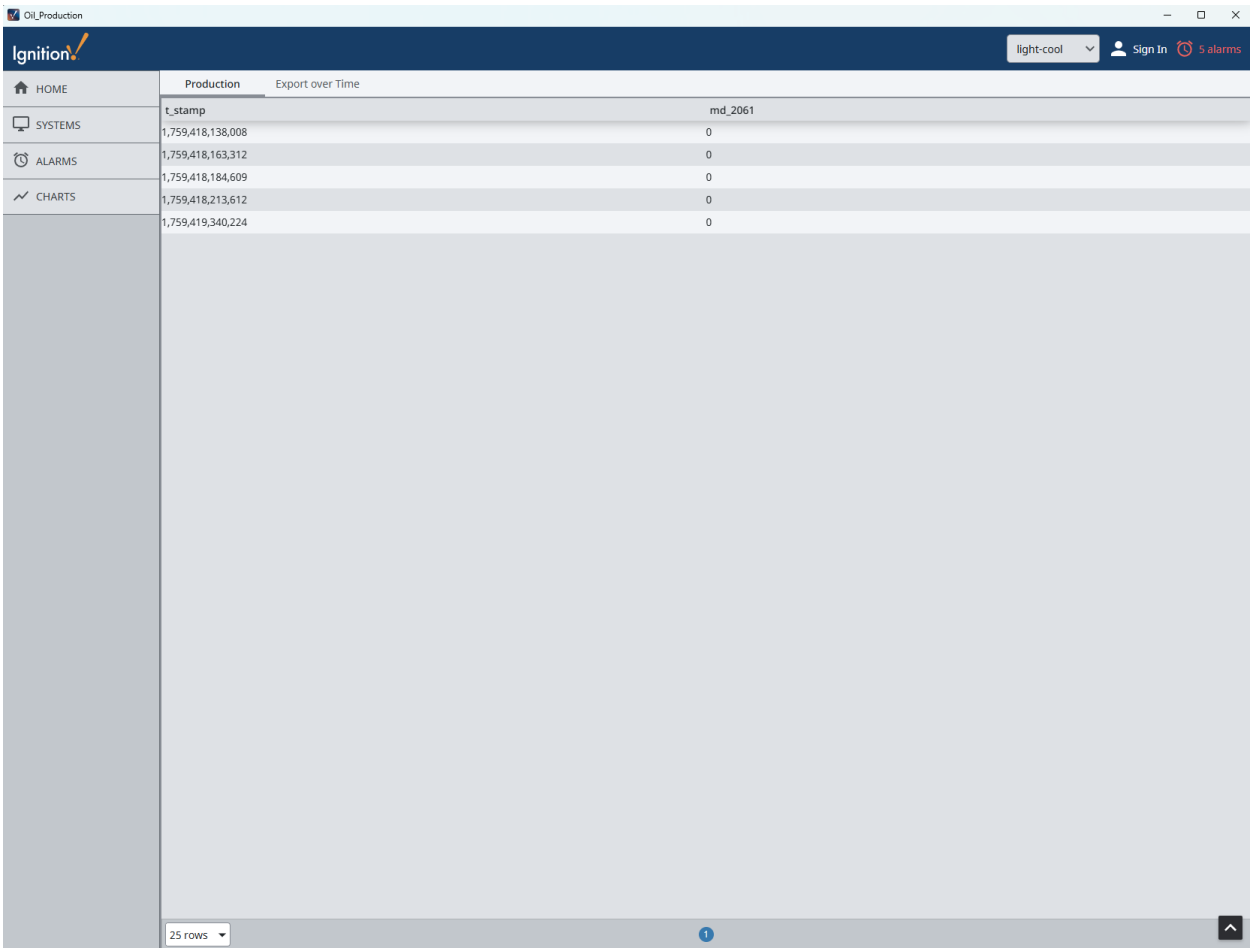




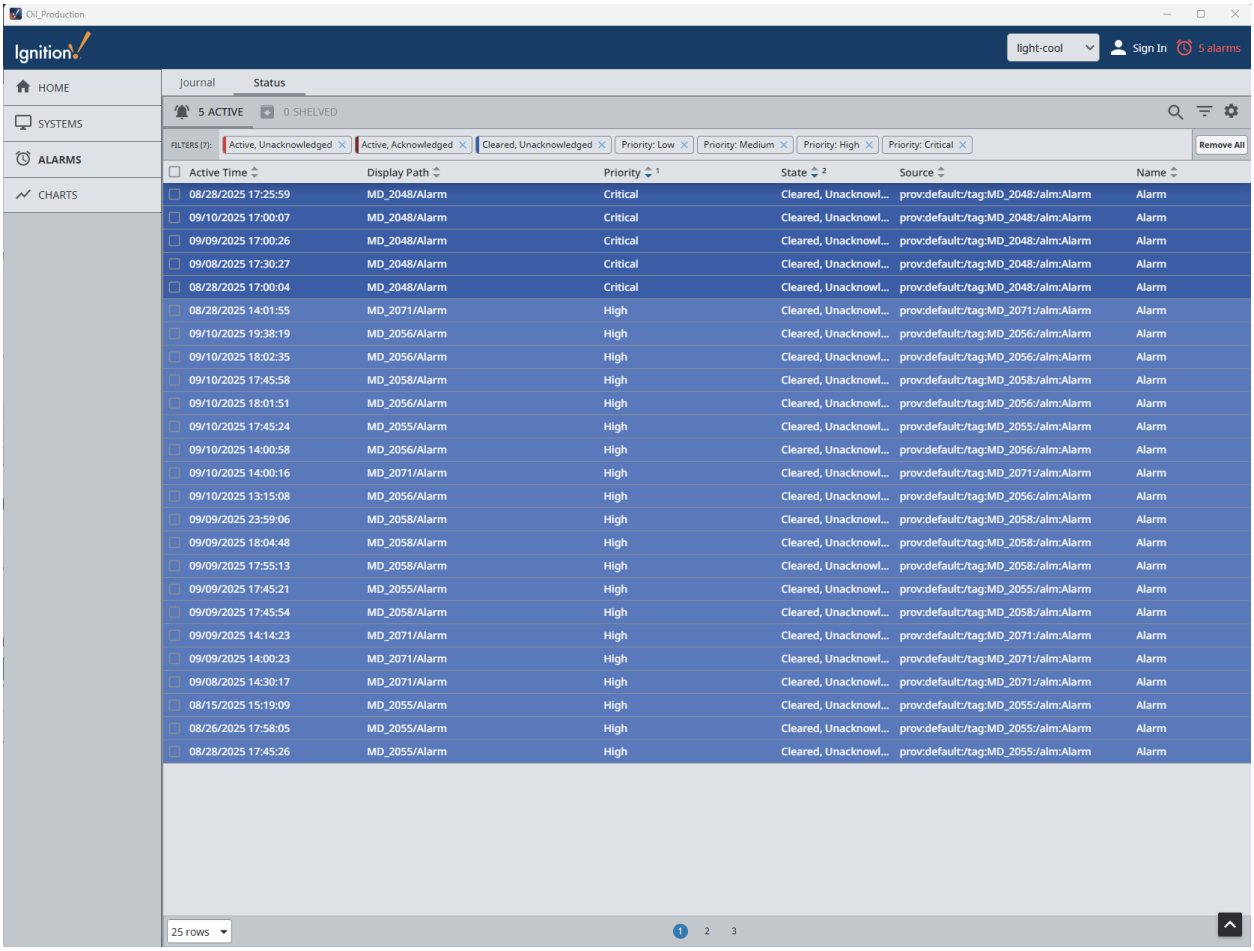
The Home page of the HMI will appear. This is where you can see the current system status as well as engage with the crane system for ICS anomalies.



The Systems page is where you can see individual sensors and engage directly with the start and stop system latches. This is also where manual override is found.

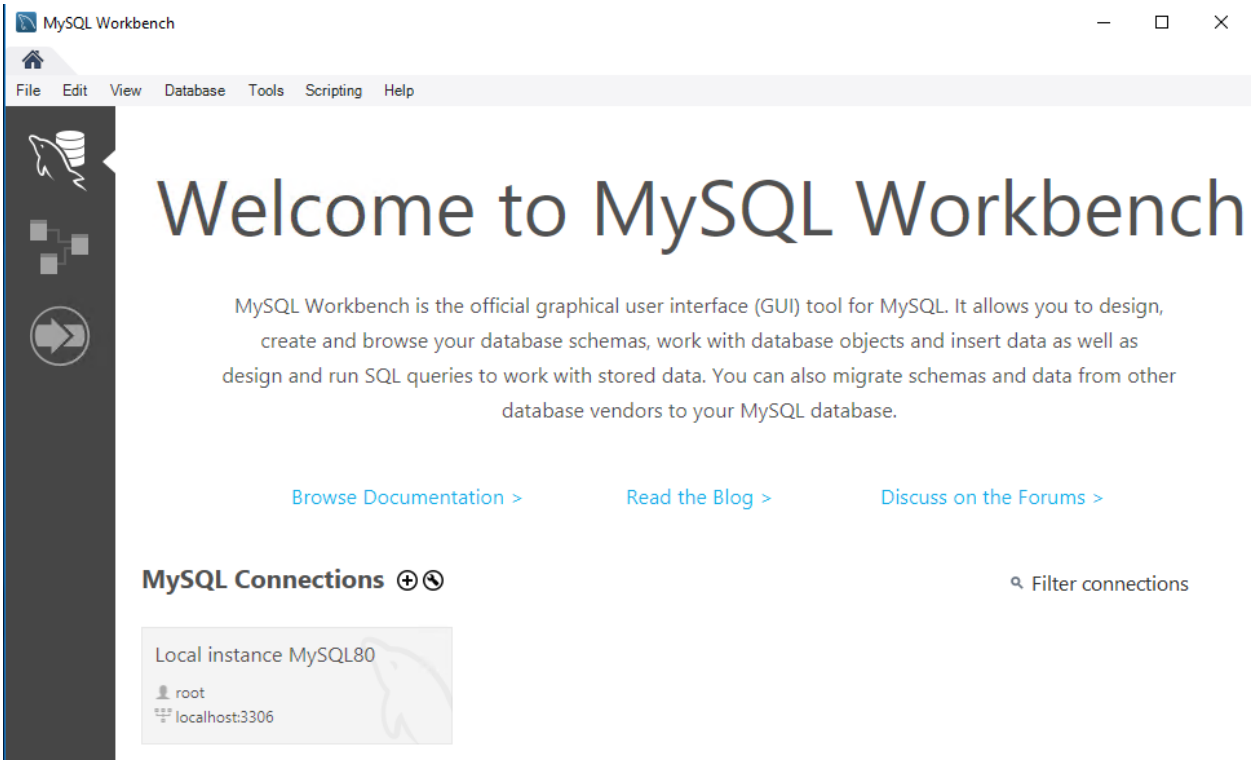


The Charts page directly corresponds to the output of the system. You can See graphical output over time, or production at specific timestamps.

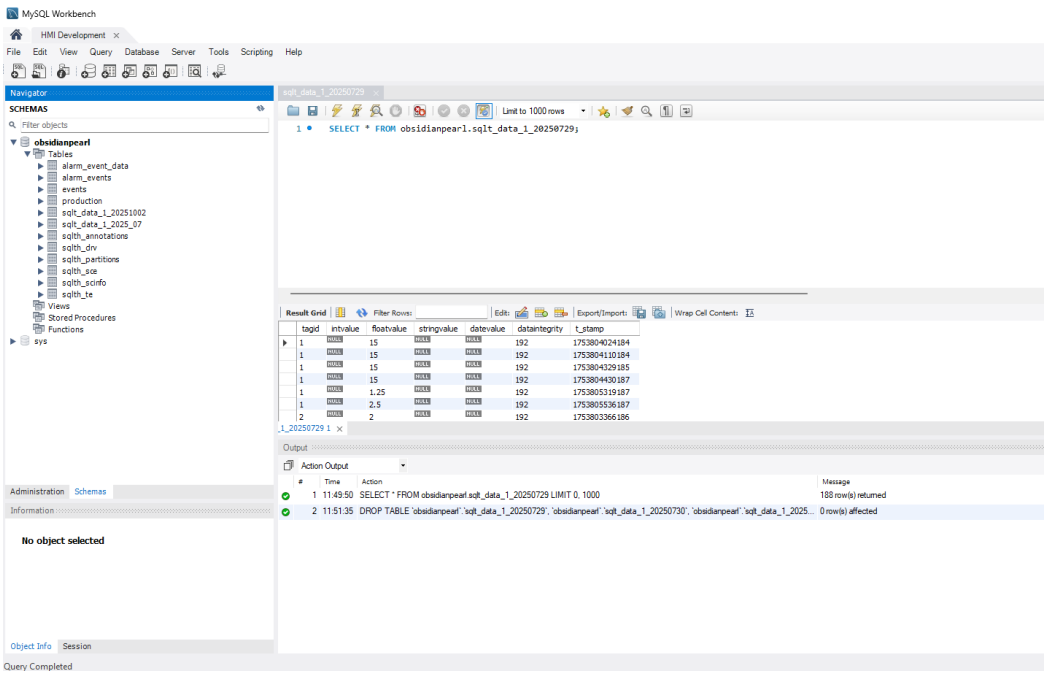


The Alarms page shows all the system alarms and provides the user the ability to acknowledge, shelf, or remove all alarms thrown by system threshold logic.

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 **blueteam: BlueTeam2025!** and should not be changed.



Below you can see the obsidianpearl database table structure breakdown.



ICS ANOMALY

Cargo Ship Resupply.

At 12:30pm and 2:45pm on competition day the cargo ship will arrive to refill the supply stock for the rig. The cargo containers must be hoisted from the ship to the rig platform within the scheduled time slot. All crane interactions can be done in the bottom righthand corner of the HMI Home page as seen below. You must be able to figure out the operations to properly communicate with the Crane controller.