IoT Process Control at the Edge

Introduction

Azure IoT capabilities offer a number of benefits to customers seeking to manage and operate embedded devices at scale but also to manage, deploy and operate Edge devices deployed to remote endpoints at scale. IoT Edge can be deployed to Windows/Linux devices running ARM/x86 processors of varying sizes up-to and including low-power compute devices like a Raspberry PI.

IoT Edge also offers some unique and powerful capabilities for industrial customers running manufacturing, inspection or control applications inside a plant. These workloads require low-latency connections to align with the tact-time of assembly/manufacturing operations and often times customers are concerned (rightfully so) about relying on WAN connectivity for their plant to operate. This is where IoT Edge can be deployed to offer value to customers needing to run, local in the plant, capabilities to support data collection, processing or to integrate as part of a closed-looped control system where close proximity to devices like Programmable Logic Controllers (PLCs) are running process control functions in a plant. Typically these customers have additional security concerns opening up industrial control system networks that are isolated by design for security reasons directly the Internet or to Internet connected services. IoT Edge can play an important role in this scenario to deploy local to a customer's environment features of Azure such as Azure functions, ML services, data collection/aggregation operations and closed-loop control applications in a secure and low-latency manner while offering the ability to manage and operate these environments at scale from the cloud.

So how can an Edge device connect to these industrial control networks? Usually these networks are specialized to the manufacturer of the PLC such as ControlNet, Profinet, Modbus and many others. For a compute device to easily communicate to these networks manufacturing plants typically employ OPC, or Open Platform Communications as a means to facilitate direct communication to industrial control hardware. This involves software from vendors such as Kepware, Rockwell Automation, Iconics, Siemens and countless others the bridge the gap between the control network and open-APIs that can be used by software to pull/push data to these PLCs running industrial applications/operations.

So how does this extend to the Azure IoT Edge space and how can this help? IoT Edge offers capabilities to run custom 'code' or commercially supported modules on the

compute appliance to perform tasks or to be triggered by an external event. Microsoft makes available Industrial IoT modules that can be deployed to IoT Edge devices deployed to plants that allow these devices to easily extract and interact or be triggered by data/state changes on PLCs using OPC! This OpenHack will involve building a solution on how this can be leveraged to solve many common engineering scenarios in the industrial control space.

Background

Contoso has a sophisticated manufacturing environment distributed across many plants in many countries. They use a number of PLCs in these plants but have a common vendor they use for an OPC/UA server to capture data for their plant historian. They would like to take advantage of real-time analytics capabilities of the cloud to stream their production process control data generated by sensors and instrumentation captured by their PLCs in the cloud. Their security team is concerned about opening their OPC server up to public internet connectivity but their quality and maintenance teams would both like to use cloud ML and time-series reporting capabilities to analyze data emitted from PLCs. Your goal as an architect is to help them plan a solution on how to safely extract this data using existing compute resources while addressing their concerns for security.

This hack includes presentations that feature lectures introducing key topics associated with each challenge. It is recommended that the host present each lecture before attendees kick off that challenge.

Duration

3 Days

Learning Objectives

In this hack you will solve common challenges for companies planning to use Azure IoT in Industrial IoT scenarios. This includes:

1. Deploying and configuring the IoT Edge runtime
2. Deploying modules to the running IoT Edge device
3. Managing/monitoring/configuring IoT Edge devices at scale from IoT Hub
4. Configuring an OPC (simulator) to generate factory data

5. Interfacing IoT Edge to the factory simulator to capture data and push to the cloud
6. Consuming data published to the cloud for analysis and reporting

Challenges

- Challenge 1: Deploy IoTHub/Edge
    - Get familiar with the basic concepts of Azure IoT Hub and Azure IoT Edge.
    - Iot Hub Creation
    - Edge Device creation
- Challenge 2: Deploy OPC Simulator
    - OPC Simulator to serve as our virtual 'factory'
- Challenge 3: Deploy Industrial IoT solution
    - Deploy Industrial IoT platform to the IoT Edge
- Challenge 4: Route messages and do time-series analysis
    - Route IoT Hub data to Event Hub
    - Route Event Hub to a time series data store
- Challenge 5: Process Steaming Data
    - Stream processing
    - Reading from IoT Hub
    - Aggregating/filtering data (querying)
    - Output data to data lake & Power BI
- Challenge 6: Deploy to devices at scale
    - Use Deployment manifests to deploy modules to IoT Edge devices at scale
- Challenge 7: Connect to Devices with Device Streams

    - Use Azure IoT Hub device streams (in preview) to connect to IoT Devices over SSH

- Close down SSH connectivity in a Firewall to confirm remote access is not impacted.