IoT-Mfg
600 S Bell Blvd, Cedar Park, Texas 78613
+1 (833) 468-6342
iot-mfg.com

White Paper

Today, We Hear Buzzwords like Cybersecurity, Edge to Cloud, and Digitization in Manufacturing...What About Legacy Strategy?

In your manufacturing facility today, there are hundreds, if not thousands of devices, meters, sensors, drives and motors. All sound familiar? Are they remotely located or not directly connected to the Distributed Control System (DCS), MES system or your Cloud Solution?

In IoT-Mfg's experience, these devices are the cornerstones of successful operations. We believe your data should drive your process strategy, not technology.

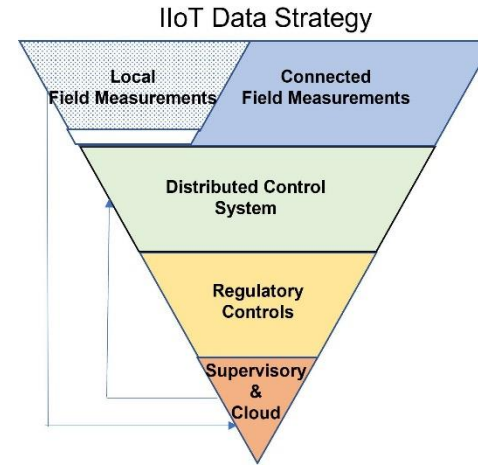
What does your data collection round look like? Is it once a shift, once a day, or even once a week? Most of these devices sit in harsh environments or are not easily powered.

All these variables are vital; each has value and is a critical piece of your IoT data strategy.

At IoT-Mfg, we believe that the plant data pyramid is upside down. The fundamental data, including variables not currently connected, are the priority. Control strategies can then advance to more complex levels once addressed.

Several other measurements might be helpful in your IIoT strategy, but what if your device locations make it impossible? What happens when running conduit and cable is no longer economical?

Take a look at the inverted pyramid.



The top layer is Local Field Measurements that are not currently connected. How do we bridge that non-connected gap in the most cost-effective manner that is robust enough for the industrial environment?

If you do a simple internet search, you will find vendors touting single application, cheap, battery powered devices.

Some IoT vendors have a very narrow view of Data. Vibration monitoring as an example is a very small slice of what your overall data strategy should be. Other vendors believe its okay that the sensor devices and gateways are battery driven and worse yet not built to be outside in your facility 24/7.

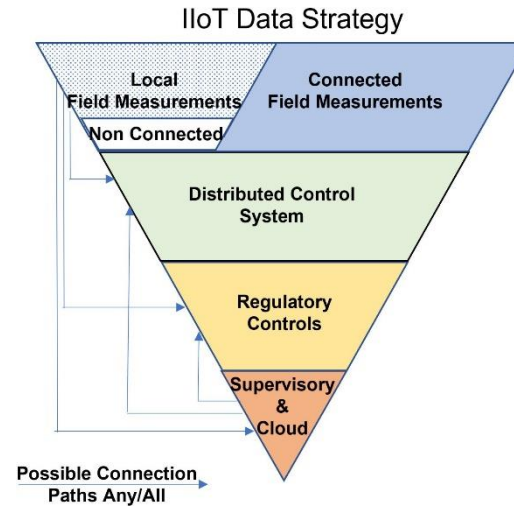
The first question you should ask is how long the batteries last. The answer, in most cases, may be a month if you want to try to use the signal in a control strategy and need to have it transmit once a minute or even once a second.

Secondly, what happens if an operator hits the transmitter with a stream of water? Often, what you will hear is don't do that. The design of the device is not equipped for harsh industrial environments.

The IoT-Mfg difference is simple, the engineering. Our devices mount in IP67- rated boxes. We provide a 12vdc power source, so battery life is never an issue. And if 115v service isn't available for the power supply, we provide solar solutions for continuous power. The transmission rate is never an issue.

The Internet of Things (IoT) is a misnomer because the devices do not necessarily need a connection to the public internet. Devices only need to be connected to a network and be individually addressable. In the Industrial Internet of Things (IIoT), there can be a connection to a remote network (cloud-based) or reside entirely within the facility's intranet.

Looking again at our inverted pyramid, notice that some communication lines have been added, the beauty of the IIoT network. Once the data is captured, how it can be used is unlimited. It is no longer necessary, or required, that all IIoT data must go to a cloud application. We see customers using this data in their MES applications or Localized PI Workbook applications.



Communication is provided by using Edge computer gateways and modems. Edge Gateways allow communication of data to popular cloud platforms such as Microsoft Azure, Amazon AWS, Losant, MQTT, and more. Modems forward data to the internal intranet using different communication formats, such as Bluetooth, TCP, Serial, RS-485, or other popular communication technology. The Edge Gateway provides both and supports cellular connectivity. The Edge computer also provides advanced computational capabilities.

IoT-Mfg does not provide any cloud services. Our approach is to capture the data and transport it into your network. An edge computer is located inside your internal DMZ and takes advantage of your established security protocols. From that point, you can filter, manipulate, transform, record, report, and generally use the data as you see fit. After all, it is your data.