Smart Factories and the Challenges of the Proximity Network

Authors:

Daniel Barnes
Director of Product Management
Synapse Wireless
daniel.barnes@synapsewireless.com

Brandon Dauphinais
Technical Writer
Synapse Wireless
brandon.dauphinais@synapse-wireless.com

1. INTRODUCTION

In the Industrial Internet Consortium's (IIC) Industrial Internet Reference Architecture (IIRA), examples of architectural patterns for Industrial Internet of Things (IIoT) are described; two of which we select for this Smart Factory discussion: the **3-Tier Architecture** and the **Gateway-Mediated Edge Connectivity and Management Architecture** (Figure 1). In both architectures IIoT gateways and edge devices form the boundaries of the proximity network. The challenges and corresponding solutions in the proximity network will be viewed in terms of this general architecture.

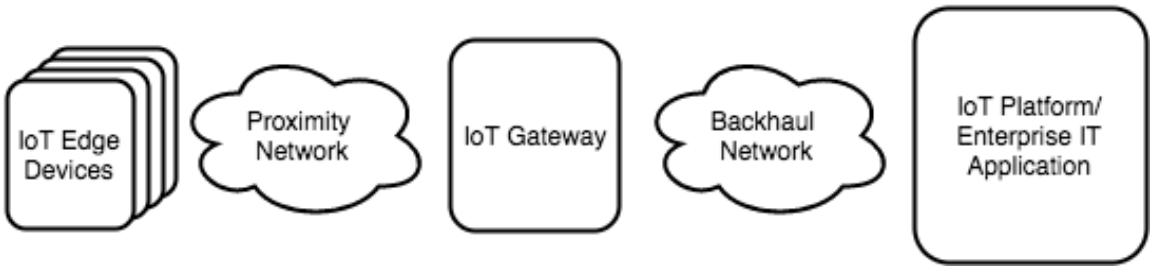

Figure 1: Gateway-Mediated Edge Connectivity and Management Architecture

As we studied the proximity network in the factory, the Synapse team noticed a prominent "progression of challenges" (Figure 2) that begins with specific use cases. Each use case creates a unique set of integration challenges that drives the selection of connection technology such as wired Ethernet, Wi-Fi or 802.15.4. The connection technology creates a secondary set of challenges that are often overlooked in the initial system design phases. We have grouped this secondary set into three general categories: Distributed Intelligence, Deployment and Long-term Management. We will focus on a subset of use cases found in the Smart Factory and follow the corresponding progression of challenges and proposed solutions.

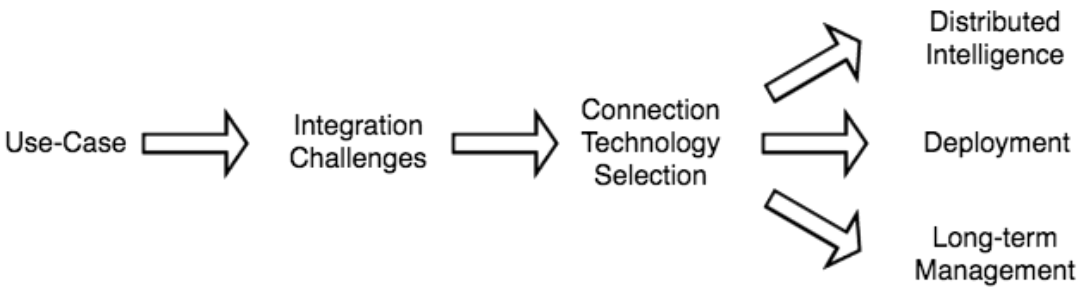

***Figure 2**: The Progression of Challenges*

2. USE CASES DRIVE INTEGRATION CHALLENGES

Based on interviews and on-site evaluations, Process Improvement and Predictive Maintenance emerge as the two leading IIoT use cases in the Smart Factory. These two will serve as the focal

point for the remainder of this discussion due to their prominence and similarities in implementation. Asset tracking for inventory management was the third-most prominent use case. However, it will not be considered at this time due to the additional integration challenges it poses such as positioning and dynamic edge device association.

IIoT in the Smart Factory integrates the physical sensors and actuators (or their Programmable Logic Controller (PLC) or Human Machine Interface (HMI)) of Operational Technology (OT) with the enterprise applications of Information Technology (IT). The use cases in the Smart Factory form the basis of these integrations. In order to fully explore these two use cases, we will examine both in the context of six integration challenges:

1. powering the edge device
2. networking the edge device
3. integrating sensors and actuators
4. integrating with IT
5. data bandwidth and
6. data reliability

Before we jump into the six major integration challenges, let's take a moment to review the two use cases of Process Improvement and Predictive Maintenance.

2.1 Process Improvement

Most factories have well established and highly efficient processes already in place. However, plant managers still focus on ways to improve their process efficiencies. In some cases, they operate in a commodity market where the business operates on a few cents of margin per unit. In other cases, the plant manager has tight deadlines or safety concerns driving the need for greater visibility into problems earlier in the process. Most of the possibilities to gain additional efficiency occur at the integration points between different automated processes. Quality and production flow need to be first understood and then ultimately controlled at these integration points.

One plant we visited processes about 50,000 lbs of chicken per day. This particular plant takes raw chicken breasts and produces a variety of finished products such as breaded chicken, cooked chicken, and sausage – all of a variety of shapes and sizes. The plant manager highlighted portion control as their key issue. Early in the process, a machine cuts the raw chicken breast. Breading and cooking processes operate on the cut chicken further down the plant line. If the chicken is not the right size and shape coming off of the cut line, then the rest of the process is flawed and they produce an unsatisfactory product. Today, problems in portioning associated with manual data recording are not discovered for 24 hours. It is much too late to address the problem and they have to start over, losing valuable time as well the cost of materials and labor. The plant managers look to solve the problem by automatically measuring weight and size as each piece

comes off the cut line and recording this information for real-time monitoring by the plant manager (Figure 3).

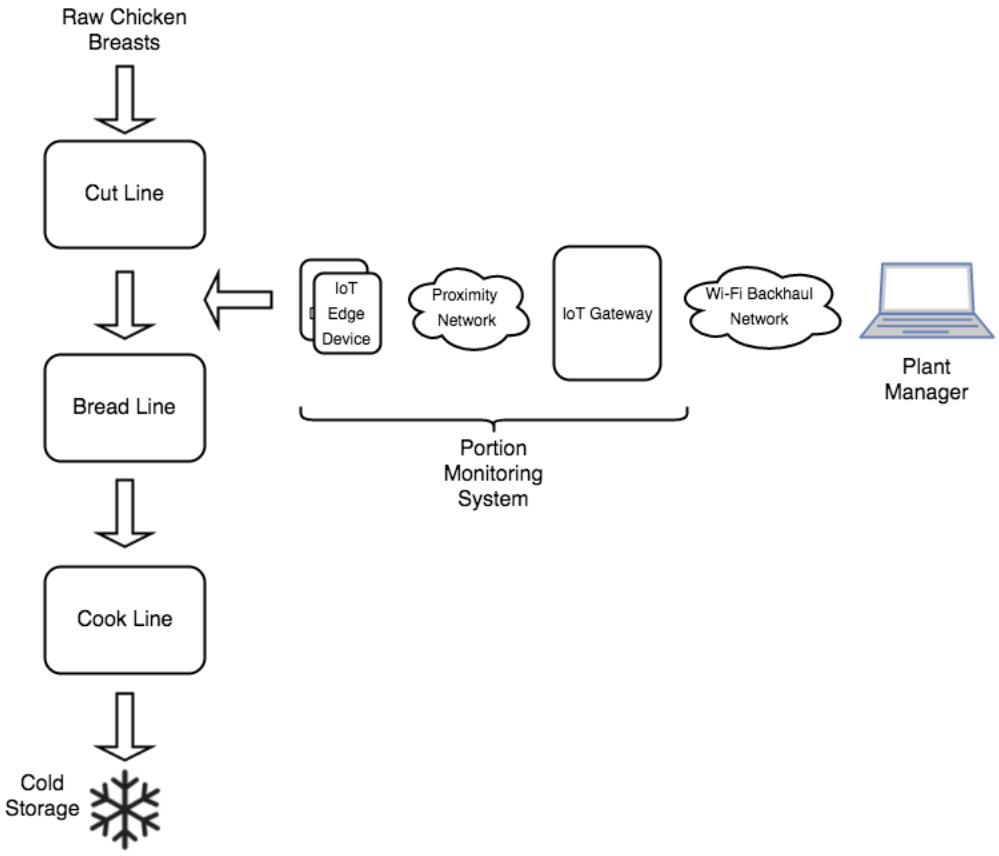

Figure 3: A Gateway-Mediated Edge Connectivity and Management Architecture at a Chicken Plant

2.2 Predictive Maintenance

While the majority of factories explore how Machine-to-Machine (M2M) and IIoT technologies improve process, few factories have been able to successfully implement predictive maintenance. Many factories have mechanisms for scheduled *preventative* maintenance and redundancy on critical systems, but few predict failure in time to perform maintenance. Predictive maintenance generally involves collecting sensor data such as temperature and vibration from critical components (such as motors) and analyzing it over time. The algorithms for detecting maintenance conditions can be as simple as threshold crossing or as complex as a trained neural network.

We have noticed two prominent predictive maintenance business models emerge. In one case, the plant integrates sensors from their critical equipment into their own systems and manages all of the data and networking themselves. In other cases, the factory consumes a piece of equipment from a vendor such as a motor in a compressor. The vendor seeks to expand its business model by offering a service to monitor its equipment.

We toured a factory that produces 17,000 fire extinguishers per day. The plant manager highlighted several systems, such as a large air compressor, that would halt plant operation if they failed. The plant manager mentioned that one day, a critical piece of equipment suddenly failed and they did noy have the spare parts available to fix it. Production was shut down for *five weeks* while they waited for parts and repair. Predicting that equipment failure could have prevented this company from having that huge profit loss.

One motor production company we interviewed seeks to expand its business model by offering service contracts on motors installed into plants (Figure 4). They want to monitor the utilization as well as temperature and vibration of their motors and collect the data remotely. This information will help them design better motors based on understanding their customers' needs while also helping them predict when failures might occur.

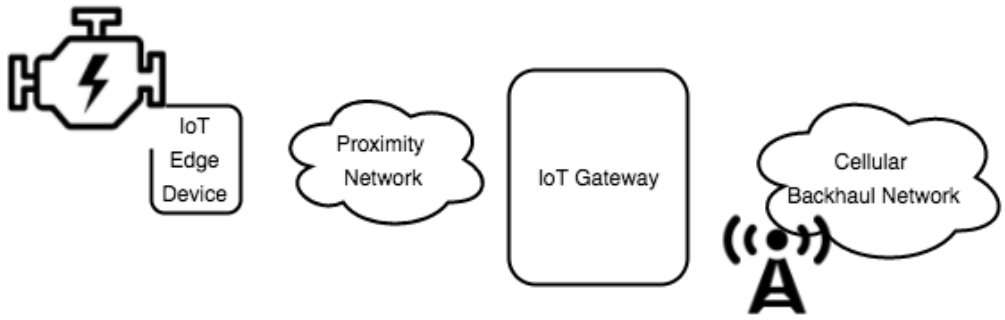

Figure 4: Monitoring a Motor for Service Needs

2.3 The Six Integration Challenges for Implementing IIoT for Smart Factories

Now let us consider how process improvement and predictive maintenance use cases are handled by considering the six integration challenges that have to be addressed when designing a solution (Figure 5).

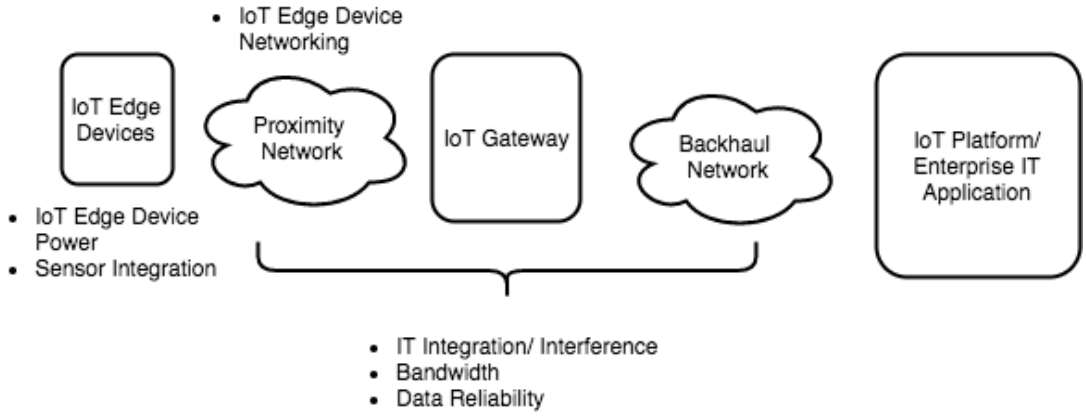

Figure 5: The 6 Integration Challenges in Relation to the Gateway-Mediated Edge Connectivity and Management Architecture

2.3.1 Powering the Edge Device

Factories typically have ample power supplied throughout the facility, often making it easy to drop power to an edge node, but this does have its cost and difficulties. The choice of battery power or wired power to the edge device is a prime influencer of the connection technology decision.

For Process Improvement

In most cases, process automation applies wired power to the edge device in the factory. For example, a factory uses dedicated power to run the robotic arm that loads the products into shipping crates. But in some cases, the edge device is hard to reach with dedicated power. For example, one factory we toured has a large furnace that runs at 2000 degrees Fahrenheit, which makes running power wires to a sensor inside the furnace a difficult and costly task, particularly when the sensor was not built into the furnace by the manufacturer.

For Predictive Maintenance

As opposed to process improvement, predictive maintenance systems are backup systems. Plant managers often pay less to have these installed or will have them installed while they are implementing a process improvement initiative. Additionally, the sensors are often mounted onto existing equipment in ways that were not originally intended by the equipment vendor. Installers typically wire power to predictive maintenance edge devices only if it is cheap and easy to do so, otherwise they look to battery-operated edge devices.

A recurring example of predictive maintenance that we have observed in our tour of factories and plants is placing vibration sensors on motors in order to predict when an engine failure is going to occur.

2.3.2 Networking the Edge Device

Most factories have wired Ethernet drops throughout the facility. In some cases, it is not cost effective to wire networking to each edge device. The use case dictates whether the edge device should have wired or wireless connectivity.

For Process Improvement

When attempting process *automation* as a means of process improvement it will usually require wired networking to the edge device for data reliability and bandwidth. Fortunately, process *monitoring* does not typically require such high levels of precision, as those involved are looking for long-term trends, which means a few lost data-packets will not undermine the solution.

Process *monitoring* use cases often desire wireless connectivity in order to avoid the costs of running network cabling throughout the factory (One factory operator said it can cost up to $1,000 per foot to run cabling to an edge device). Also, some process monitoring needs to be done on objects than cannot be easily wired. For example, in a chicken processing plant, the

plant workers used handheld probes to take measurements of chicken portions on the process line. To improve process monitoring, the factory replaced manual recordings of the measurements with digital records that would transmit to a centralized database. Given that the probes were handheld, a wireless solution was necessary.

For Predictive Maintenance

The reasoning applied to powering applies even more so to networking. As many of the devices factory and plant operators need monitored for maintenance will have to be retrofitted for monitoring, it is very likely for predictive maintenance edge devices to be wirelessly connected. One case we have seen of this was the desire to monitor an engine of a crane in a ductile iron factory. Giving its inherent movement, connecting a wired sensor to monitor it would have been unfeasible. Instead, the factory placed a wireless, battery-powered vibration sensor on the crane motor and began collecting data to predict when the engine would need servicing.

2.3.3 Sensor/Actuator Integration

There are a variety of different physical sensor interface types, such as 4-20 mA, RS-232 and 0-10 volt with a variety of different protocols for interfacing to sensors and calibration parameters for interpreting the data. The IIoT system architect must decide where and how often the interpretation occurs.

For Process Improvement

The edge device will likely be purpose-built for each application as it will either integrate with an existing interface (such as MODBUS) or be designed as part of a new piece of equipment. The specifics of the application will drive where conversions take place. For example, one factory we toured has a brazing furnace inside of which they want to install a temperature probe. The probe uses a 4-20 mA interface connected to a wireless transmission unit.

For Predictive Maintenance

If the application is a retrofit of existing equipment, then the edge devices likely interface to external sensors, typically via 0-10 V or 4-20 mA connection. Fortunately, most modern factory equipment comes designed via a PLC that can be connected to via MODBUS.

Finding a system that can easily integrate with both existing factory equipment (with PLCs) and new edge device sensors is the key challenge. For example, the crane monitoring solution mentioned previously was part of a larger effort from the factory's IIoT architect. The architect needed to ensure that the vibration sensors' means of transmitting data could easily be funneled into the same database that held the data being collected from many of the factory's existing PLCs.

2.3.4 INTEGRATING WITH IT

Though often not a purely technical consideration, IT integration drives much of the technical decisions in the IIoT system architecture. In some cases, the IT department wants the edge devices directly integrated with IT. In other cases, they do not. In some cases, they allow data to leave the premises. In other cases, they will not. The commonality between these scenarios is that IT wants to understand and mitigate the interference an IIoT system has with their system.

For Process Improvement AND Predictive Maintenance

When developing process improvement and predictive maintenance solutions, the nature of IT integration depends largely on the size of the operation. For smaller operations, we have noticed that IT/OT generally work together smoothly and may even be run by the same department. For those where IT is a corporate entity spanning multiple facilities, plant managers tend to avoid IT during the proof-of-concept phase in order to try out their idea without waiting for IT approval. We noticed that in the case of the chicken plant, that the IIoT architect preferred using a non-WiFi based wireless solution as it allowed him to avoid having to tie into IT's infrastructure and it also avoided interference issues of WiFi-dependent devices already in operation.

Once they attempt to make their solution mainstream, IT often wants to make sure the application integrates with their existing infrastructure. In many cases, the plant is sensitive to data leaving their facility, many times due to customer requirements. One plant we interviewed would not allow data to the leave the plant because of the security concern expressed by one of their customers, the U.S. military.

2.3.5 5. DATA BANDWIDTH

The use case drives the amount and rate of data that needs to be moved to and from the edge devices. Networking technologies such as 802.15.4 may excel in low power, but do not have the bandwidth to support certain use cases like wired Ethernet and Wi-Fi.

For Process Improvement AND Predictive Maintenance

In most cases where the process is primarily being monitored at integration points, the amount of data moved per edge device is much less than 1 Mbps. In cases where feedback and control are tightly coupled, the data rate can be much higher. This design challenge is tied directly to the *powering the edge device* and *networking the edge device* challenges, as the nature of what is powering the edge device affects which methods of networking are possible.

Many of the monitoring cases we have seen for process improvement and predictive maintenance have relatively low bandwidth requirements. For example, the monitoring of the motor vibration sensor for the crane, while it requires high sample rate over a short period of time, the overall bandwidth usage is low.

But that is not always the case. The fire extinguisher factory has a video monitoring program that can detect dangerous gases and warn staff of its presence, even highlighting the area where the gas is detected. Given it is transmitting video, the bandwidth requirements are significantly higher.

2.3.6 DATA RELIABILITY

Certain use cases require a high-degree of data reliability between the edge device and the enterprise application, whereas others are less sensitive. High reliability can be achieved with many technologies, but some have more proven and easier-to-implement mechanisms to achieve robust data transfer. There is typically a tradeoff between low power and ease of reliability implementation.

For Process Improvement

The process improvement for data reliability depends greatly on the criticality of each data point being correct and the amount of automated control. For applications that are gathering data over time to look for trends (the chicken plant, for example), the reliability requirements are generally around three 9's. For applications where decisions are made automatically on the latest data point, reliability is paramount.

For Predictive Maintenance

Since a predictive maintenance system analyzes trends of data over time to produce a result, some data loss is more tolerable than in many process improvement use cases.

3. INTEGRATION CHALLENGES DRIVE CONNECTIVITY DECISIONS

The IIoT System Architecture provides three discrete connectivity decision points (Figure 6): the sensor/actuator interface, the proximity network and the backhaul network. The various integration challenges directly impact the choice of connectivity at each of these interfaces.

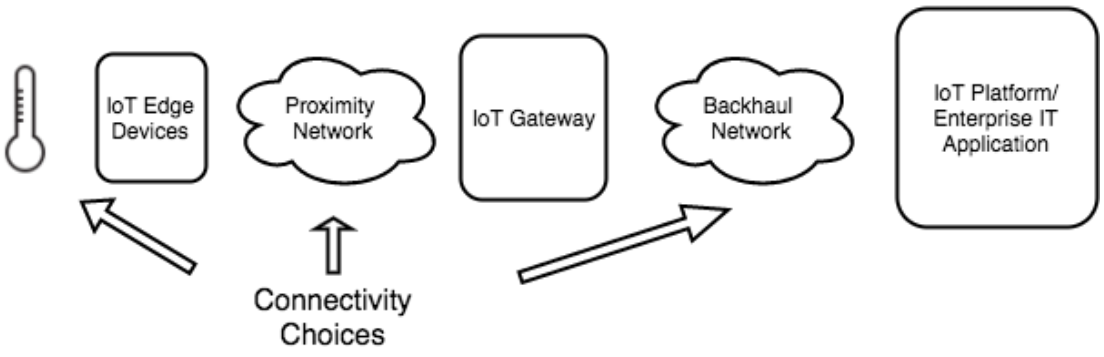

Figure 6 : Three Connectivity Choice Points

3.1 Sensor/Actuator Interface

The sensor/actuator interface is the physical and logical interface between the sensor/actuator and the IIoT Edge Device. The following integration challenges have direct bearing on how this interface is chosen.

Powering the Edge Device – Wired-power devices allow for a much wider range of sensors and simpler hardware integration efforts. Battery-operated devices require tight control over sensor/actuator current draw.

Sensor/Actuator Integration - This consideration is extremely application-specific. Consider these three unique cases:

- The edge device reads an ADC value from a 4-20 mA temperature sensor.
- The edge device samples a vibration sensor 1000's of times per second and performs a fast Fourier transform (FFT).
- The edge device must implement or at least transport a higher-order protocol such as MODBUS.

The hardware (and resulting software) integration of the sensor often represents a significant portion of the development cost and time.

3.2 Proximity Network

There are a variety of connectivity options in the proximity network. We will focus on wired Ethernet, Wi-Fi and 802.15.4 technologies. We have seen these technologies cover various sets of integration challenges well, though there are certainly other technologies that could work in this environment.

Powering the Edge Device - If wired power is available, wired Ethernet, Wi-Fi and 802.15.4 are all viable technologies in the proximity network. The remainder of the integration challenges must be considered to make a good choice. However, if the edge devices are battery operated and the batteries need to last for a long time (measured in months or years) without replacement, then 802.15.4 is the better choice.

There are three primary power consumers on the edge device: Radio Frequency (RF) communication, the processor and the sensor/actuators. Power utilization is controlled by disabling the bulk of the power consumption in these three areas for extended periods of time. Typical battery-operated devices wake-up for a very short period of time to read a sensor, perform minimal processing and then transmit the data. Then they go into a low-power sleep mode. 802.15.4 is built for this particular low-power model due to its ability to very quickly transmit a single piece of data and then go to sleep. Wi-Fi takes time to lock onto an AP and typically runs an uncompressed Internet Protocol (IP) with additional RF overhead.

Networking the Edge Device - The decision to use wired Ethernet over Wi-Fi or 802.15.4 dictates much of the downstream considerations such as distributed intelligence, deployment and long-term maintenance.

Integrating with IT - If IT requires integration with the IIoT network there are really two choices. Either the edge devices use the existing IP network to communicate with the gateway or the integration occurs at the gateway and the edge devices operate in a separate network. 802.15.4 and Wi-Fi can both operate in the 2.4 GHz frequency space. There are mechanisms, such as using specific channels, to keep them from interfering, but this must be considered at design time. Additionally, there are 802.15.4 solutions that run over a 900 MHz carrier frequency that will not interfere.

Data Bandwidth – Two key characteristics of a communication technology is the maximum bandwidth and maximum transmission unit (MTU). 2.4 GHz 802.15.4 typically runs at a line rate of 250 kbps and uses packet sizes of 128 bytes. Wired Ethernet and Wi-Fi support much higher data rates and typical Ethernet MTU sizes.

Data Reliability - Applications typically use the well-proven mechanism of TCP/IP over wired Ethernet or Wi-Fi for data reliability. Although Transmission Control Protocol (TCP) can be run over 802.15.4 it is very undesirable for low-power applications. It requires precious RF time to create a connection and then utilizes a significant portion of each 128-byte packet just for transport. In this case, reliability is typically implemented with a different mechanism much more like reliable UDP. Some robust implementations contain a powered set of 802.15.4 repeaters that store information sent by battery-operated devices for reliable gathering. 802.15.4 provides the ability to mesh so that the communication network can more easily work around obstacles and heal when a particular link is interrupted.

3.3 Backhaul Network

The backhaul network is considered in this paper as it dictates a large portion of the gateway functions, in turn affecting the proximity network. The backhaul network typically runs IP over wired Ethernet, Wi-Fi or cellular.

Integrating with IT - If IT integration is desired then wired Ethernet or Wi-Fi is typically used. The gateway is given an IP address on the internal network and may not even send data outside of the local IT network. For those cases where IT integration is not desired, cellular is used. This is sometimes problematic and cellular coverage can be unreliable in certain locations.

Data Bandwidth - The bandwidth needed in the backhaul network is directly related to the amount of data sent/received to/from the edge devices plus any additional management traffic.

Data Reliability - TCP is used ubiquitously in the backhaul network for data reliability.

4. DISTRIBUTED INTELLIGENCE

IIoT is often viewed as dumb edge devices that spout data into a cloud instance for deep learning and processing. Real applications often require more distributed intelligence such that decisions are made where the right context and processing power exist. There is the need to not only distribute intelligence to the IIoT Gateway but even to the IIoT Edge Device (Figure 7).

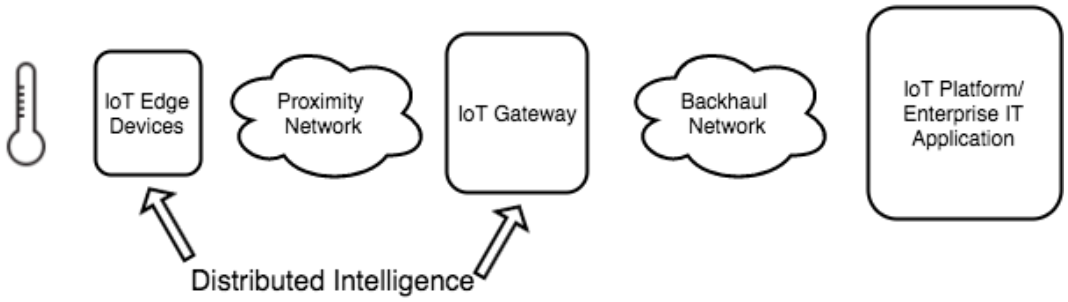

Figure 7: Two Areas of Distributed Intelligence in the Proximity Network

4.1 IIoT Edge Devices

Every use case requires some level of software in the edge device. Integration challenges and the choice of connectivity determine the complexity of the software and the corresponding developer skill set.

Powering the Edge Device - Wired power devices can often take advantage of an embedded Operating System (OS) such as Linux. However, on battery-operated devices, these heavyweight OS's often will not work due to the time it takes for them to wake as well as the limited RAM and Flash space on these constrained devices. Additionally, these devices require specialized software on the edge to manage the power duty cycle. The software manages the sensors, processes the data and then forwards the data on. It then shuts everything down in a low power mode. Wake can be controlled by external events or via a schedule.

Networking the Edge Device - The edge device will require a networking stack and the ability for an application to read a sensor and transmit the data over the network.

Sensor/Actuator Integration - Even the simplest sensor integration such as reading a General-purpose input/output (GPIO) pin requires some software. In many cases, the edge device integrates with the sensor through a full protocol stack such as MODBUS. The edge device often has the best context for interpreting a raw sensor reading into something meaningful such as degrees Fahrenheit.

Data Bandwidth - For limited bandwidth applications, the edge device may be programmed to only send data when a threshold is crossed or send an average of the data over time.

Data Reliability - The network stack on the edge-device is necessary to implement reliable data transfer. In the case of battery-operated devices, the application on the edge needs to be much smarter to reliably transmit data.

4.2 IIoT Gateway

The IIoT gateway plays an important role in distributing intelligence in the IIoT application due to its location as a proxy between the edge devices and backhaul. Additionally, it generally carries more processing power than edge devices allowing for an increase in local decision making.

Powering the Edge Device - Battery-operated devices generally need the higher horsepower of the gateway to aid in the reliable data collection. In many instances, software on the gateway coordinates the sleep/wake periods of the edge devices and ensures that data is reliably delivered.

Integrating with IT - The gateway provides a prime location to shield the IT department from the networking complexities of the edge network. It can do this in the form of protocol conversion or in the form of presenting the sensors and proximity network as a service to IT. As IIoT becomes more prevalent, we will likely see the proximity network, gateway and edge devices less as a point solution and more as a service to be shared among multiple applications.

Data Bandwidth - The gateway also manages the utilization of the backhaul network. Cellular backhaul in particular often requires aggregation logic on the gateway such as summing and threshold-crossing detection to limit the utilized bandwidth.

Data Reliability - The gateway can play a key role in data reliability not only for battery-operated edge devices, but also for wired-power devices. In cases where the backhaul network is unavailable, the gateway can maintain the data collection and even some of the application logic until connection is restored.

5. DEPLOYMENT

In many cases, the IIoT solution design considers the connectivity and development concerns, but fails to account for deployment until the solution is being installed. The choices made on connectivity and distributed intelligence drive the set of deployment issues.

5.1 Connectivity

The networking approach in the proximity network dictates much of the deployment problems. Wired Ethernet often requires electrical work and some IT work for switch setup. Wireless installation often requires some site survey to make sure that signal strength and interference are at appropriate levels. Additionally, the edge devices must have the correct security credentials and networking parameters provisioned to make them easy to install securely. These credentials can be programmed at manufacturing time or via an installation application or some combination of both.

Wi-Fi and wired Ethernet have a well-developed set of deployment capabilities. 802.15.4 on the other hand presents a set of difficulties unlike those of Wi-Fi and wired Ethernet. 802.15.4 can often have a mesh topology bringing greater reliability, but also increased difficulty in setting up paths through the network. There are tools available to view the mesh topology and corresponding signal strengths to help identify single points of failure and weak links in the network.

5.2 Distributed Intelligence

Once IIoT Edge Devices and Gateways are placed and networking is established, the software needs to be distributed and configured. In some cases, the edge devices and gateways are programmed with the correct software at manufacturing, but often the software needs to be upgraded or configured at the time of install. The proximity network needs to provide the capability to upgrade and configure the edge devices and gateway without direct physical access.

6. Long-term Management

The IIoT solution is not complete upon install. Changing conditions in the physical world sometimes cause unreliable data sources and failed IIoT devices. In addition, the solution may need to be upgraded with a new feature, bug fix or security patch.

Wireless networks will drop traffic at times and IIoT devices will die. A robust solution will not only detect failures, but also aid in pinpointing the root cause. For example, if the gateway is driving reliable data collection, it can also report when an edge device fails to respond. There also needs to be mechanisms to troubleshoot networking issues such as ping, trace-route, topology views, signal strength views, etc.

Typical OS's such as Linux allow the user application to be upgraded independent of the underlying OS, network stack and drivers. This creates a great deal more robustness in the upgrade process. Typical embedded software is treated as "firmware", i.e. software that isn't upgraded often or remotely. IIoT Edge Devices, however, often need a mechanism to be upgraded remotely and securely. It would be very desirable to upgrade the "user application" logic separate from the networking logic even on these edge nodes to limit the possibility of bricking the units.

7. Conclusions

The proximity network and the corresponding IIoT gateway and edge devices represent much of the complexity in building out a full Smart Factory solution. There are solutions to this complexity, but they must be picked by first considering the use case and various integration challenges to help choose the connectivity technology. Once the connectivity technology is chosen, there remain the problem sets of distributed intelligence, deployment and long-term management that must be considered during the design phase of a solution.

- Return to IIC Journal of Innovation 3nd Edition landing page for more articles
- Download the IIC Journal of Innovation 3nd Edition