RAD

Your Network's Edge®

How to Choose the Right Industrial IoT Gateway

The complete guide to selecting the Industrial IoT gateway that is right for your project size, deployment strategy and geographic spread.

Introduction

In industrial IoT (IIoT) environments, smart edge device ranging from load breakers and meter concentrators to sensors, CCTV cameras, traffic monitoring and control units, remote PLC controllers, and other automation-enabled devices are connected to the operational network and control center via an **IIoT gateway.**

The most talked about benefit of IIoT is the shift of focus to increased efficiency and lower costs using smart edge devices and Big Data analytics. Still, massive data transmissions to and from many IIoT devices in remote sites, over diverse network connections and in a timely manner are not trivial challenges to overcome. Also challenging is the need for actionable information (in other words, real-time analytics) to make sense of all the data collected.

The powerful Edge Computing IoT combination is one, very compelling way to go about it.

> *The addition of Edge Computing capabilities to the Industrial IoT gateway hardware is currently viewed with great interest as it allows the Industrial IoT gateway to perform local storing and processing of data, meaning higher reliability, lower latency and tighter security.*

So, if you're planning your new Industrial IoT project, after choosing your smart edge devices, IoT applications, management, and dashboards, you will probably want to consider the parameters by which to select the Industrial IoT gateway solution that is right for your project size, deployment strategy and geographic spread. To save you some valuable research time, we've listed below some aspects that have been found to be relevant in almost all the projects that we've been involved in. We believe they'll be useful for you as well.

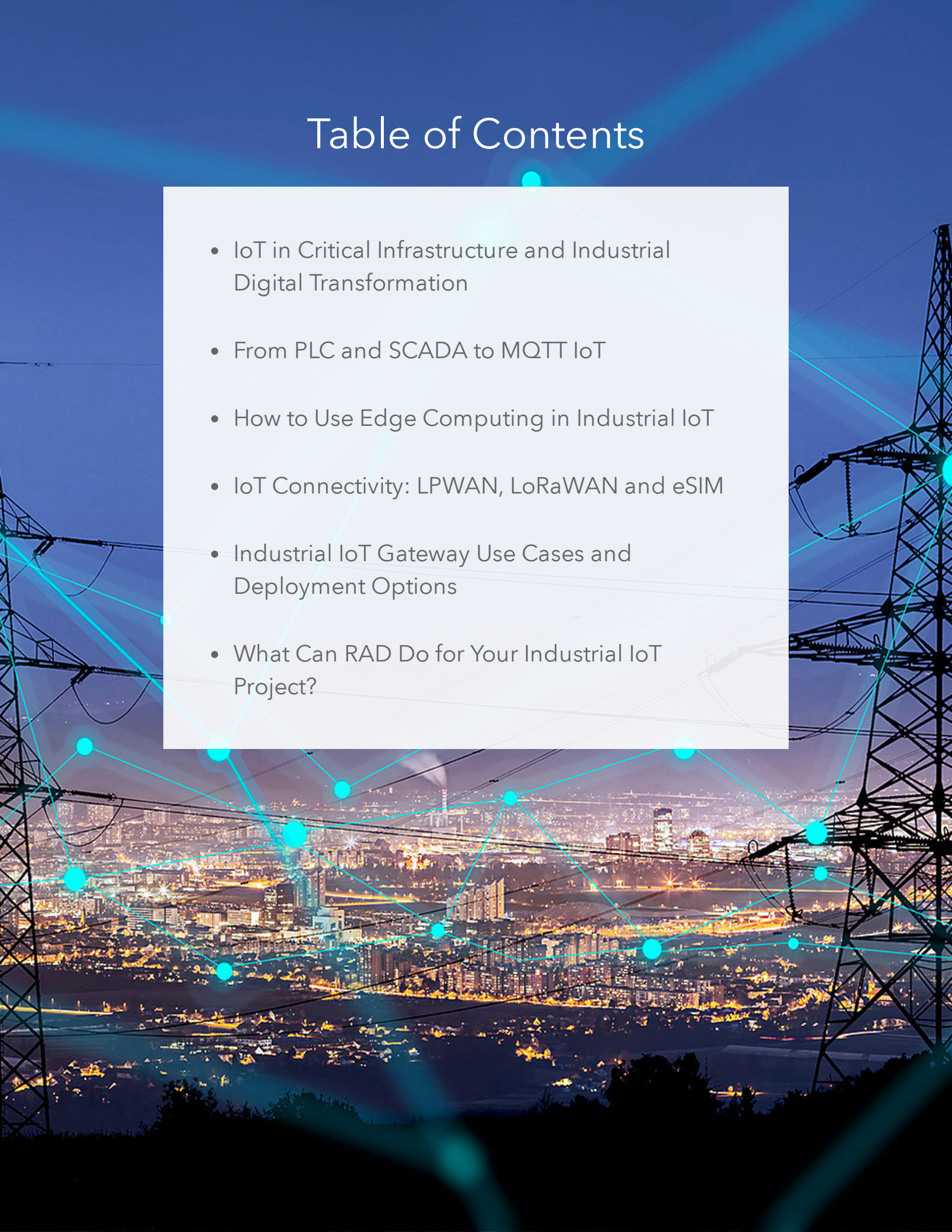
There are five widely acceptable criteria for choosing the right Industrial IoT gateway:

- Open standards
- Flexible architectures
- Cloud technology
- Edge Computing
- Cheaper and more flexible hardware

The combination of these criteria is meant to enable increased efficiency and lower costs and involves new technologies as LPWAN for IoT LoRA and LoRaWAN gateway, Industrial IoT Edge Computing, MQTT for IoT, and IoT PLC gateway for IoT SCADA.

Scroll down to read the review of all these new IIoT technology tools.

Table of Contents



IoT in Critical Infrastructure and Industrial Digital Transformation

The IoT revolution enables automation and monitoring of sensors and systems like never before – not only at a larger scale, but also with a much wider geographical coverage. Its industrial internet of things (IIoT) flavor affects the traditional utilities and industry verticals. The entire critical infrastructure sector, from power, gas and water utilities to smart cities and transportation systems is now undergoing its own digital transformation with quite powerful new capabilities.

This table attempts to list some of the many types of IoT "things" that are relevant to each of these sectors:

Power Utilities

- Smart Grid
- Re-closers
- Load breakers
- RTUs/SCADA
- Secondary substations
- Meter concentrators

Smart Cities

- Smart parking
- Traffic monitoring & control
- Bike sharing
- Smart lighting
- Public safety
- Payment kiosks (PoS)

Connected Industry

("Smart Factory")

- Production floor monitoring
- Remote PLC control
- Automated quality control

Transportation

- Traffic control
- Info boards
- Kiosks

Water Utilities

- Flow control
- Quality
- Leakage detection
- Pump/valve control
- Meter sensors

Gas Utilities

- Flow meters
- Volume/pressure/ level sensors

As you can see, they are completely different in functionality and purpose and require very different solutions to meet their very specific needs. But despite this huge disparity, they do share some common aspects. For example, they all go through accelerated adoption of IoT, Edge Computing and automation. They all gradually move to the cloud to benefit from the higher efficiency and scalability it offers, and all make growing use of Big Data and analytics. They also share increased awareness to cyber security threats in the IoT era.

> *New technological advancements and open standards are changing entire supply chains, reducing costs and making rollout times shorter than ever.*

It's also important to note that such modern IT paradigms (cloud, MQTT and Edge Computing) can be used not only for new Industrial IoT deployments, but also to augment existing legacy systems. Below is a review of key elements that ultimately affect your choice of IIoT gateway.

Not sure which technologies to consider in your indusrial IoT project?
We've collected some interesting insights that could help you make the right decision.

Contact Us

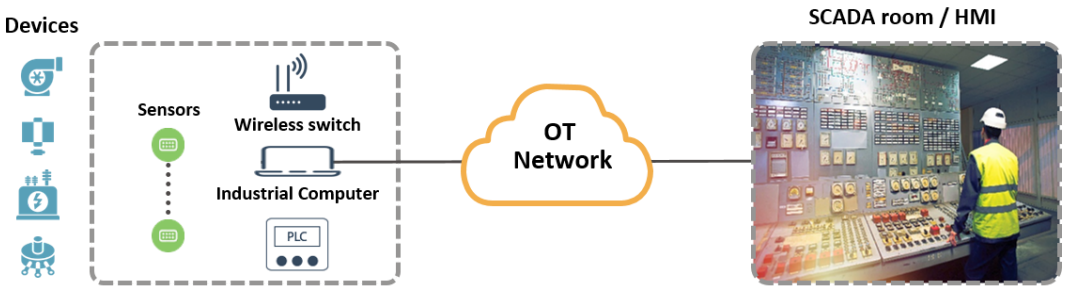
we'll happily share them with you.

From PLC and SCADA to MQTT IoT

Almost every manufacturing and critical infrastructure operation relies on an industrial control system (ICS) to operate and manage its core processes. Broadly speaking, an ICS is made of three basic entities:

- **Devices:** Programmable logic controller (**PLC**), also called remote terminal unit (**RTU**)
- **Control:** Human machine interface (**HMI**)
- **Language:** Supervisory control and data acquisition (**SCADA**)

Here is a typical representation of these entities:



On the left side, we see the types of machinery that are used in the industrial process. Some examples of these devices are pumps, re-closures, load breakers, CCTV cameras, traffic monitoring and control unit, and meter concentrators. They are often unmanned and need to be remotely controlled. Moving to the right, we see the sensors that send data on the operation of the machinery to the remote operators. That information is communicated to the control room (on the far right of the diagram) over an operational technology (OT) network. It helps the operators decide what modifications, if any, need to be made to the process. The way this is actually being done is by a central program – an HMI, or human-machine interface – that aggregates the data from the field and enable remote intervention. To help the operators in their tasks, we have the program logic controller – the PLC – which is located near the sensors.

The PLC enables the reading and interpretation of sensors. It activates and monitors machines that are distributed in hundreds, thousands and even tens of thousands remote locations. The language by which all these entities are communicating is called SCADA – supervisory control and data acquisition. SCADA has actually become synonymous with the entire ICS field. There are a number of SCADA flavors, depending on industry, geography and other factors. DNP3 and IEC-104 are two examples of SCADA protocols that had become standard. There's also a variety in PLC types, ranging from Nano and Micro PLCs to medium and large ones.

This set up is not new and in fact has been around for decades. The increased levels of automation, and IoT is a clear reflection of that, means that there are A LOT more devices ("things") to control. It also means that there's a need for new, more effective ways to rapidly deploy better ICS systems with more efficient operations, and at a lower cost.

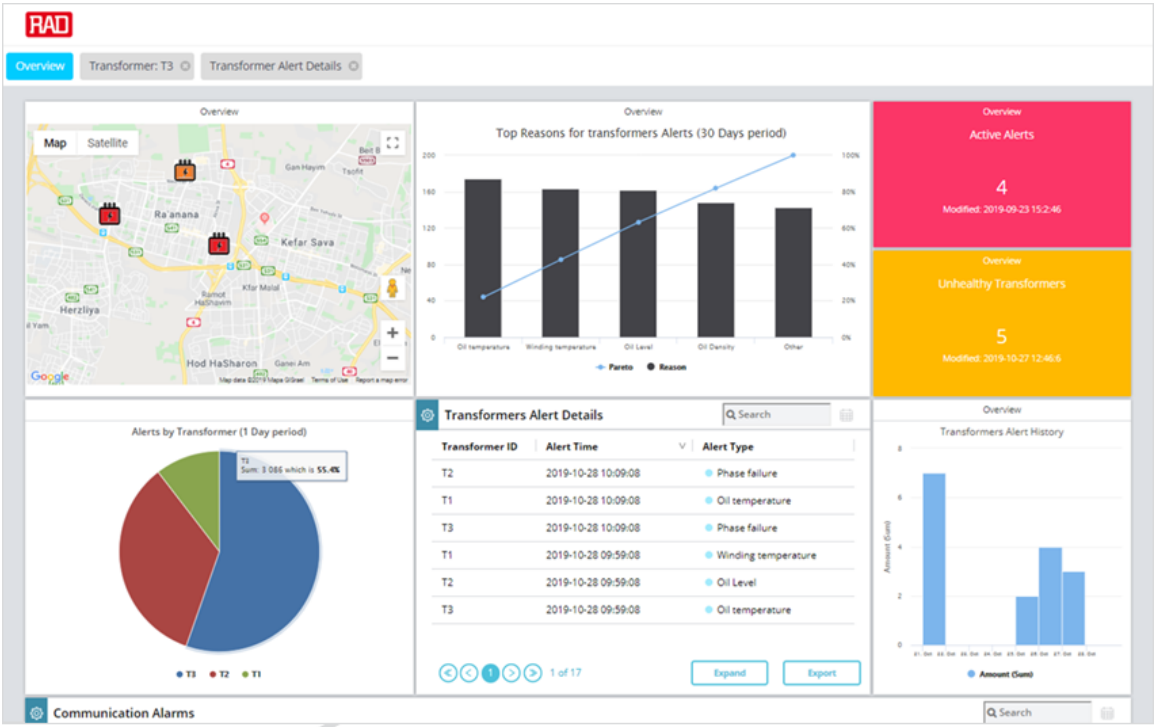
> *In other words, there's a need for new, more effective ways to rapidly deploy better ICS systems with more efficient operations, and at a lower cost. In other words, there's a need, among other things, for IoT PLC and IoT SCADA.*

The latter, IoT SCADA, is achieved with MQ Telemetry Transport, or MQTT. This M2M/IoT connectivity protocol, which originated from the veteran IBM MQ Series is, in fact, the new SCADA infrastructure. The combination MQTT IoT is considered a natural fit because of MQTT's lightweight publish/subscribe messaging format and its ability to work well even if there are link interruptions or latency issues between the PLC and control room. Many of the major cloud IoT platforms – Microsoft Azure, AWS IoT Core, IBM Watson, Google CloudIoT, and PTC Thingworx – are using MQTT to enable modern cloud-based IoT dashboards to replace traditional HMI architectures.

> *Since there are still plenty of legacy SCADA RTUs around, a hybrid IoT project where only part of the network is switched to newer technologies is quite common.*

In such cases, we'd see the older SCADA protocols that these devices use mapped onto MQTT so that they wouldn't be left out of the IoT dashboard.

These cloud-based dashboards are critical for IoT decision makers. As the key purpose at the core of digital transformation is to drive efficiency by making informed decisions fast, any IIoT solution must include a tool that would display the status of the network in the context of the target key performance indicators (KPI), error alters, etc. In the IoT dashboard below we can see what key information is typically presented, in this case for a power grid. There's a geographical map showing where the power transformers are located, a time-based trend of transformer alerts and their causes, a status indication of active transformer alerts and transformers with possible performance issues, historical view, and a list of active alerts that need addressing.



How to Use Edge Computing in Industrial IoT

Edge computing is a cloud environment located closer to automation-enabled devices at the edge of the network rather than at the data center. These “end points” are connected to the operational network and control center via an IIoT gateway. The addition of cloud computing resources to the IIoT gateway at the edge enables local storing and processing of data, which, when compared to centralized cloud computing, Industrial IoT Edge Computing offers compelling benefits that are hard to ignore:

- **Higher reliability:** Because data doesn’t need to travel to a central cloud, communication isn’t interrupted if the link is down
- **Lower latency** and consumption of network resources, for the same reason
- **Letter security** and compliance with regulation as data isn’t exposed when traveling over public links

Cloud computing and virtualization enable multiple applications to run simultaneously and independently on the same hardware. In the context of IIoT, this means that a single IIoT gateway can perform not only networking functions, as has been its original purpose, but also host other functions that are related to industrial applications and IIoT management.

The end result is less “boxes”, as less networking and IIoT devices are required. This also means better security as the function that needs to be secured is virtualized within the securely connected IIoT gateway itself. All this means that Edge Computing provides the required insight and agility, and at the same time reduces the number of devices that need to be deployed in remote sites.

Where Edge Computing comes into play in new IIoT projects:

Project Parameters	Requirements
New applications with modern dashboards	Protocol conversion (from legacy SCADA to MQTT)
100s, 1,000s and 10,000s new edge points	New PLCs (for new sensors and ICS)
Hybrid or greenfield – legacy SCADA + MQTT sensors and PLCs or all new	LTE or other wireless backhaul
	= 3 boxes at the edge (1,000s of nodes)?

New IIoT projects are most likely driven by the Industrial IoT application or applications that the organization is looking to introduce. These are accompanied by one or more relevant dashboards to provide operators with the information that they need to react quickly to anything that goes on in the field. The rest of the project is built around this initial decision. Many new edge points need to be deployed across a wide geographical area to provide the necessary data.

This set up could be built from scratch ("Greenfield") with brand new MQTT-enabled sensors, or added to an existing installed base of legacy SCADA device, which would require a protocol convertor to enable the machinery and sensors to "speak" with the dashboard. In addition to new IIoT PLCs, this project would also require some form of wireless connectivity – LTE or other – to backhaul the data between the IIoT sites and the control room (wide geographical coverage, remember?). So theoretically, three separate boxes are needed in each remote location. Now let's multiply this by the number of sites (hundreds? Tens of thousands?) and we end up with a massive footprint that would prove to be a nightmare to manage and maintain.

With Industrial IoT Edge Computing, on the other hand, we're cutting down these numbers by a factor of three, as we'll see below.

IoT Connectivity:

LP-WAN, LoRaWAN and eSIM

Let's say that you're looking to deploy a multitude of new IIoT sensors in new sites – measure humidity in an agriculture environment, or detect pollution in a Smart City project – but these sites aren't equipped with power cabinets to provide electricity for these sensors.

That's a problem. The solution?

Switch to low-cost, **battery operated** sensors. Ideally, such batteries should be able to run on for years. The data from such sensors is aggregated into the cloud, so that the logic is in the cloud, but the low-cost Industrial IoT sensors are everywhere.

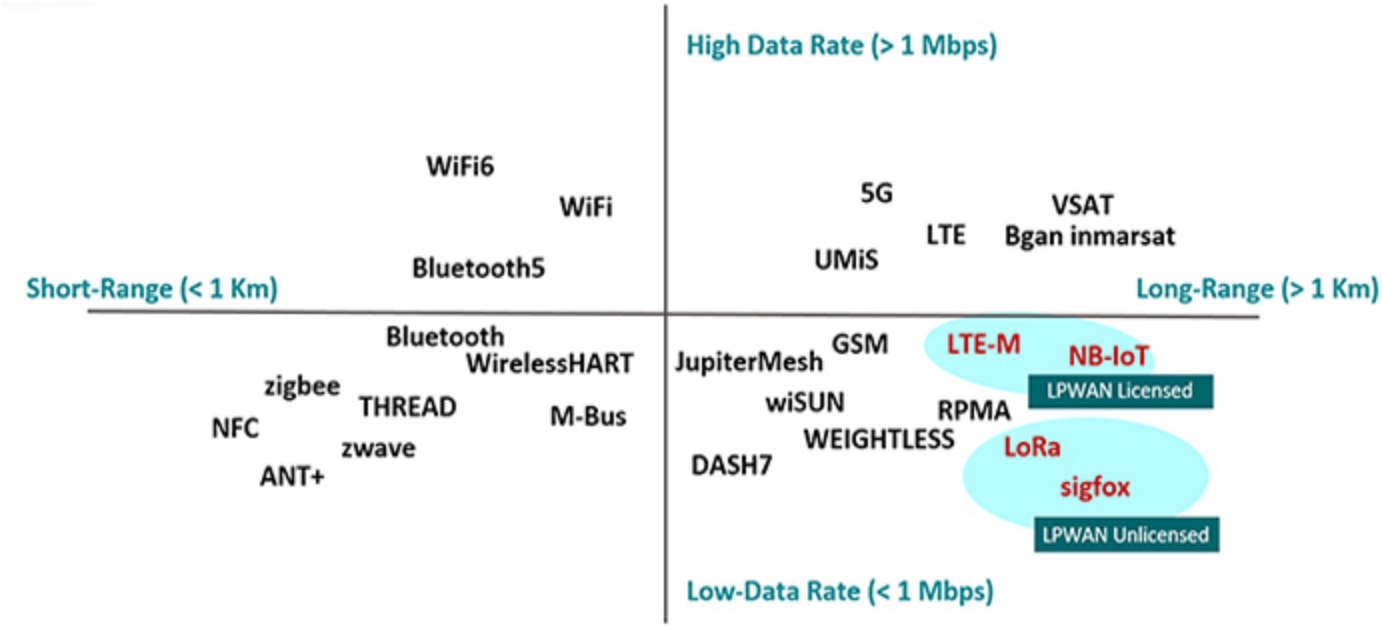
For this to happen,

you'd probably want to use a Low-Power Wide Area Network, or LP-WAN. LP-WAN is a wireless wide area network technology that connects low-bandwidth, battery-powered IoT devices.

Here are its main highlights:

- Sensors with a battery that lasts 3-6 years
- Aggregation sites with a 5 Km (3 Miles) radius and LTE (or other uplink to the cloud)
- Low bit rates (so you wouldn't consume huge amounts of bandwidth) over long ranges
- Supports many connected devices over a large area
- Low cost, high power efficiency

To give you a better idea of where you'd find LP-WAN in relation to other wireless WAN technologies, here's a helpful map:



As you can see, **LP-WAN** flavors appear in the bottom right quadrant of low range (typically above 1 Km (about 0.6 Miles) and low data rate (below 1 Mbps) technologies, which represent the "sweet spot" for this application. Within the LP-WAN spectrum, we can find licensed and unlicensed technologies. The most popular unlicensed technologies today are LoRa (Long Range) and sigfox, while in the licensed M2M LP-WAN category we find LTE-M and narrowband IoT (NB-IoT).

The most notable difference between these categories is cost. Obviously, unlicensed technologies are more economical than licensed (cellular) ones, although LTE-M is not as expensive as "regular" LTE. But there are other differences which you would probably take into account when deciding on your most suitable choice. The table below summarizes these key differences between licensed vs. unlicensed LP-WAN:

Unlicensed (Non-cellular)		**Licensed** (Cellular)
LoRa, sigfox	Key Technologies	NB-IOT, LTE-M
Very Low	Cost of battery operated sensors	Low
Very Low	OpEx	High
Required	Base station infrastructure	By Telco
None	Dependency on mobile operators	Full
74% (LoRa) 148% (sigfox)	Growth in past year*	53% (NB-IOT) 79% (LTE-M)

* Source: IoT Analytics Research

Today, LoRa and sigfox's battery-operated sensors are priced below the ones which work with cellular technology. Another capital expenses item is the base stations infrastructure – you would need to assume this cost if you're going for unlicensed wireless technology, such as IoT LoRa, but in a licensed option this would be provided by the telco operator, as would everything that has to do with your IoT connectivity, meaning a full dependency. On the other hand, the operating expenses (OpEx) in unlicensed IoT LoRa and sigfox are lower as there are no recurring costs to the operator.

When it comes to licensed cellular IoT connectivity, there's another important aspect to note – the extremely low flexibility in working with a single cellular operator. There are a number of implications to this if the IIoT project in question spans large or international areas:

- Lack of full coverage by a single operator
- Operators are using regular SIM cards with fixed international mobile subscriber identity (IMSI)
- SIMs with local roaming are driven by the originating operator
- Cumbersome configuration and management
- Any change requires physical SIM replacement and device configuration

So if the project parameters are relevant, you might want to consider a universal IIoT eSIM. Those available today already support LTE-M and NB-IoT, they are carrier-agnostic and can be remotely managed Over-the-Air to change the electronic provider profile when switching telco providers.

So what can be done with all these new tools?

Industrial IoT Gateway Use Cases and Deployment Options

Let's take a look at how different projects are coming together by adding these new technologies to the Industrial IoT gateway.

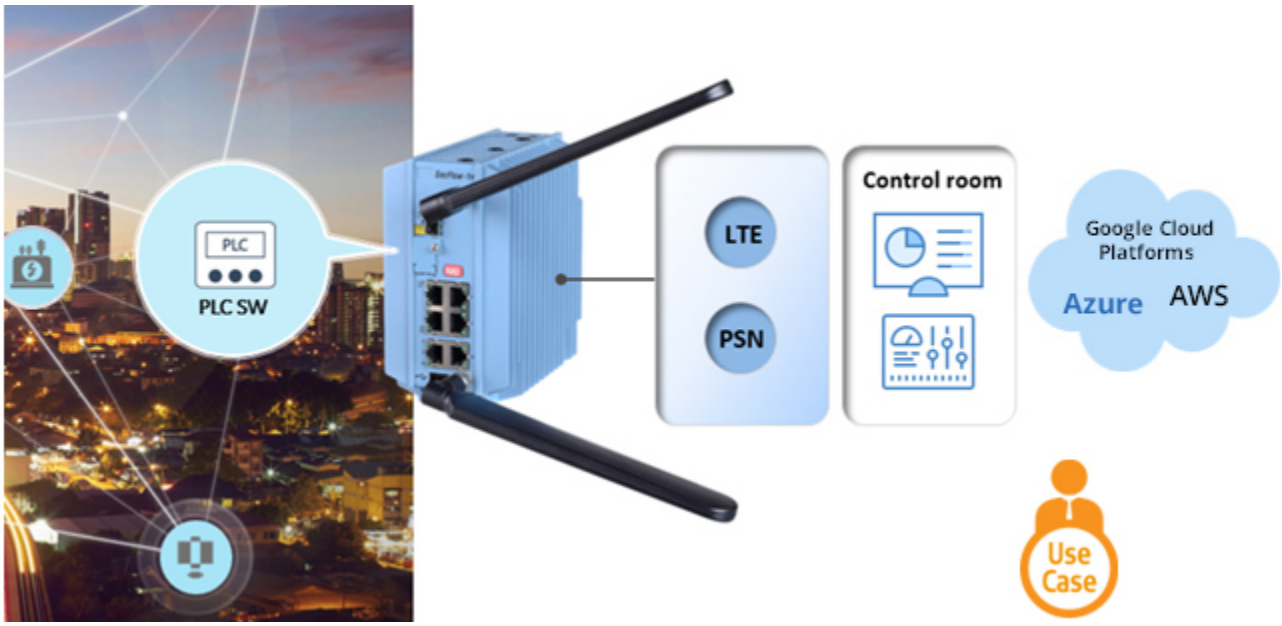
Less Boxes, Better Security:
IIoT Gateway with a Built-in PLC

PLC software can be added to the IIoT gateway using Edge Computing and, when combined with analog and digital inputs/outputs, turning it into a PLC IoT gateway and making the external PLC redundant. In this case, the PLC IoT gateway is a combination of an LTE router, PLC and industrial PC. HMI users can use intuitive dashboards to remotely control all units in the field and adjust the operation of sensors and relays as necessary.

Recommended capabilities for the PLC IoT gateway include:

- SCADA firewall IPS/ADS, stateful firewall IPsec, OpenVPN and PKI, Anomaly Detection
- PLC ladder logic; Master/Slave inter-connectivity options
- Northbound interface to HMI/dashboard
- Protocol support: Modbus, DNP3, BACnet
- Protocol conversion to MQTT

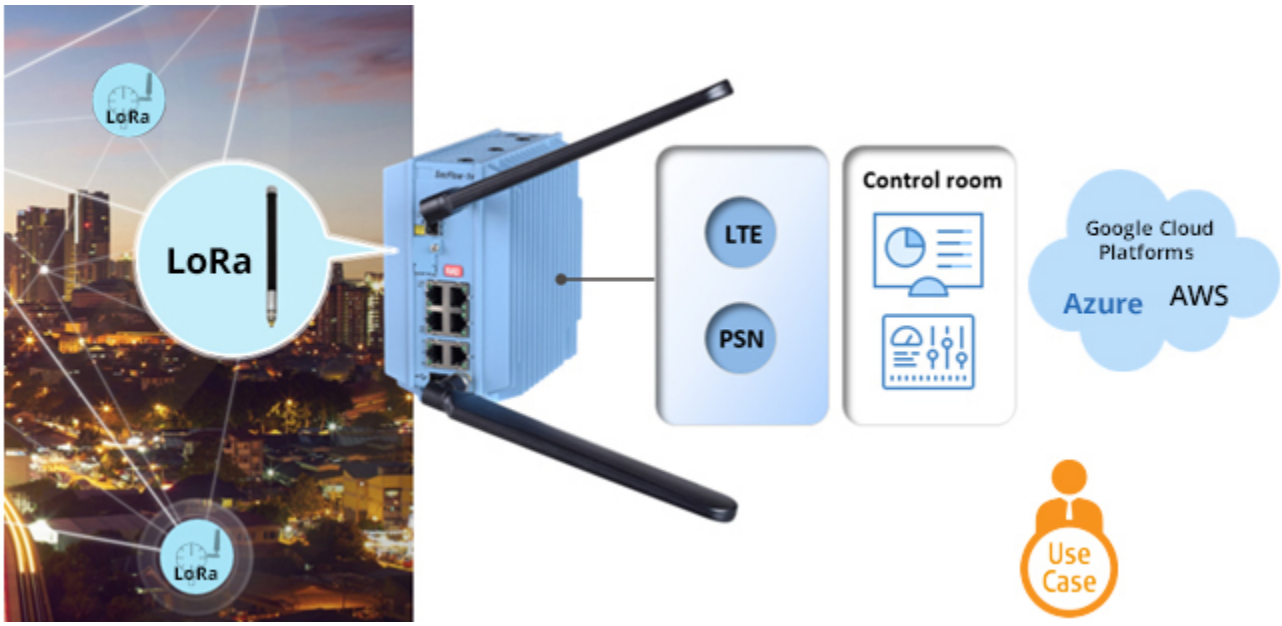
Here is an example of the PLC IoT gateway would look like:



Complete Wireless Coverage:
IIoT Gateway with a Built-in LoRa Base Station

The IIoT gateway can also be turned into a LoRaWAN gateway. By enhancing it with license-free LoRa LPWAN technology it can be used to connect large volumes of low cost LoRa sensors and meters, aggregate their data and securely deliver it to cloud servers via fiber, Ethernet, 3G/ LTE cellular or unlicensed microwave radio. The LoRaWAN gateway is essentially a hybrid licensed (LTE) and unlicensed (LoRa) solution.

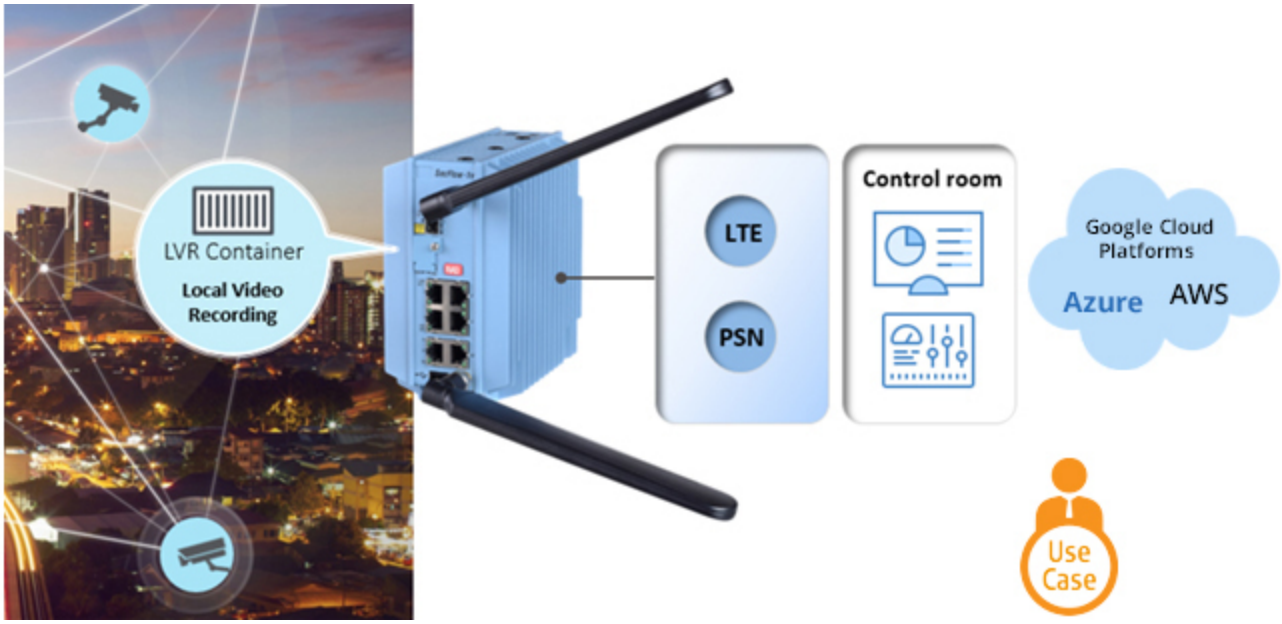
In this case, the LoRaWAN gateway would look something like this:



BYO-GW – Build Your Own (IIoT) Gateway

When you need to customize your own solution, embedded Edge Computing provides you with an open platform (specifically, LXC/LXD on ARM) and intuitive development environment to add various industrial IoT applications as edge computing virtual machines.

Essentially, you can create your own IIoT gateway according to your specific needs:



So, if you're planning an Industrial IoT project rollout, make sure your IIoT gateway includes Edge Computing capabilities. Why? You'll cut down the number of devices you need to deploy and earn higher reliability, lower latency and better security when transferring data to and from multiple remote sites. Most importantly, you'll get the flexibility you need to customize your solution to fit your project parameters.

What Can RAD Do for Your Industrial IoT Project?

To help you with your Industrial IoT (IIoT) roll out, we offer ruggedized, multiservice and compact IIoT gateways with Edge Computing, a VPN aggregator and advanced security information and event management (SIEM). RAD's IIoT solution hosts both networking and non-networking functions on the same hardware, to reduce the number of devices in the network and increase security and reliability.

The **SecFlow-1v-LoRa**, for example, leverages license-free LoRa LP-WAN technology for water and power utilities, smart cities, transportation and many other verticals. It collects data from LoRa sensors and meters and securely delivers it to cloud servers via fiber, Ethernet, 3G/LTE cellular or unlicensed microwave radio. LoRaWAN eliminates wiring, is easy to deploy and does not need any licenses. It reduces the energy consumption of connected objects while giving them years of autonomy by exchanging small data at low speed.

If it's PLC functionality you need, there's the **SecFlow-1v-PLC**. It features PLC capabilities and makes the external PLC redundant. This has a two-fold advantage: Less boxes and overall better cyber security, as no one can physically access the PLCs since they are fully contained within the IIoT gateway. With built-in security and high-availability for applications controlling mission-critical operations, it presents an all-in-one solution for automation applications in the oil and gas, water and power utilities, industry 4.0 and building automation sectors. Securely connect digital inputs and outputs, analog inputs, Ethernet/IP or serial RTUs, cameras, and more over LTE or fiber networks – either public or private.

SecFlow-1v highlights include:

- Hosting of third-party software using container technology
- Multiservice support: GbE copper and fiber, serial, Power over Ethernet (PoE)
- Single or dual cellular mode, dual SIM
- Dynamic routing and secure VPN
- Full cyber security suite
- Serial protocol handling with transparent tunneling/protocol conversion/terminal server
- Zero-touch provisioning, firewall configuration, fault management and reporting
- Digital and analog IOs with integrated RTU/PLC functionality
- LoRaWAN gateway for remote sensors aggregation
- IEC 61850-3, IEEE 1613 and EN 50121-4

Go to SecFlow-1v online >>

Not sure which IIoT gateway you need?

Talk to us – we're happy to help!

RAD
Your Network's Edge®