Preddio Technologies™

Understanding IoT

A Comprehensive Guide for Industrial and Commercial OEMs

Understanding IoT is for OEMs that are new to the Internet of Things (IoT) but need to digitize their business. In today's Internet connected world, understanding the "what and why" of IoT is critical, but equally important is the recognition that there is no one size fits all approach. Armed with this information you will be better equipped to evaluate and specify the right IoT solution to meet your business needs.

To Start - What is IoT?

The Internet of Things (IoT) has matured into a set of common technologies and deployment strategies. Most often IoT is defined as a network of physical objects—"things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet (Source: Wikipedia). IoT, by definition, always includes a connection to the Internet and in most cases a cloud-based application captures, analyzes, and displays the operating conditions of physical assets. Data from sensors is transmitted to the cloud for storage, analysis, and visualization. IoT solutions are commonly used to predict mechanical failures of physical assets in industrial or commercial environments. By connecting to the Internet, IoT solutions are able to leverage vast computing resources that would not normally be available to on-site sensors. At a high level, the fundamental building blocks of most IoT systems include:

1. Sensors

One or more sensors are used to gather information from equipment, physical assets, processes or activities that are of interest. Sensors can include basic temperature, pressure, flow, voltage, vibration, and frequency (although more sophisticated sensors such as optical, navigational, or inertial are often utilized). In the example diagram to the right, a pressure sensor is reading a value of 40 pounds per square inch (PSI).

2. Electronic Conversion

An analog to digital converter (ADC) on a printed circuit board (PCB) translates information from the pressure sensor into a format which can be digitally transmitted. Without diving into the details, in this example the pressure sensor has a signal output of 4 volts which the ADC recognizes as the integer number 40, which corresponds to a value of 40 PSI, which is then represented in binary form as 101000 (machine language).

3. Transmission

The binary value captured from the sensor is encrypted for security reasons (or should be) and is sent from the on site computer network via the Internet to a remote cloud computer or data center. Data transmission most often takes place at regular time intervals based on the application needs, or sometimes only when there is a significant change in the sensor's value.

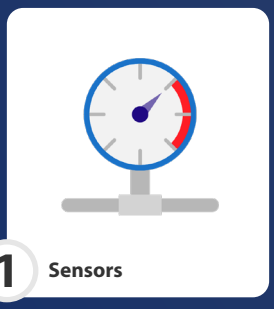
4. Data Storage

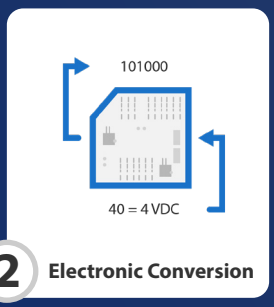
After reaching its final destination, the sensor value is typically stored in a computer database that can easily serve other systems (hence the name "server"). From here there are vast opportunities to implement data security, retention, redundancy, reliability, and user access policies.

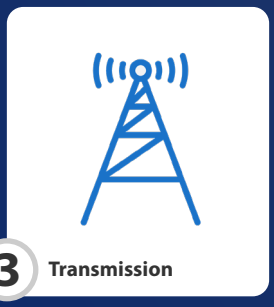
5. Web Visualization

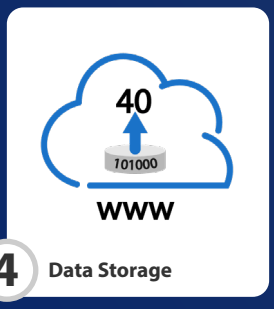
For humans to visualize the sensor information, typically a user interface (UI) is built on top of the database to display the sensor data in a chart or report. Often these user interfaces are built using a programming language called hypertext markup language (HTML) and are viewed in a web browser or via a companion mobile app. Since this information is now accessible remotely via the Internet, an unlimited number of creative applications can be created anywhere in the world. Operating at nearly "real-time" across vast distances, the visualization of sensor data for the masses is an incredible benefit enabled by IoT.

Preddio Technologies™









But why would you need IoT?

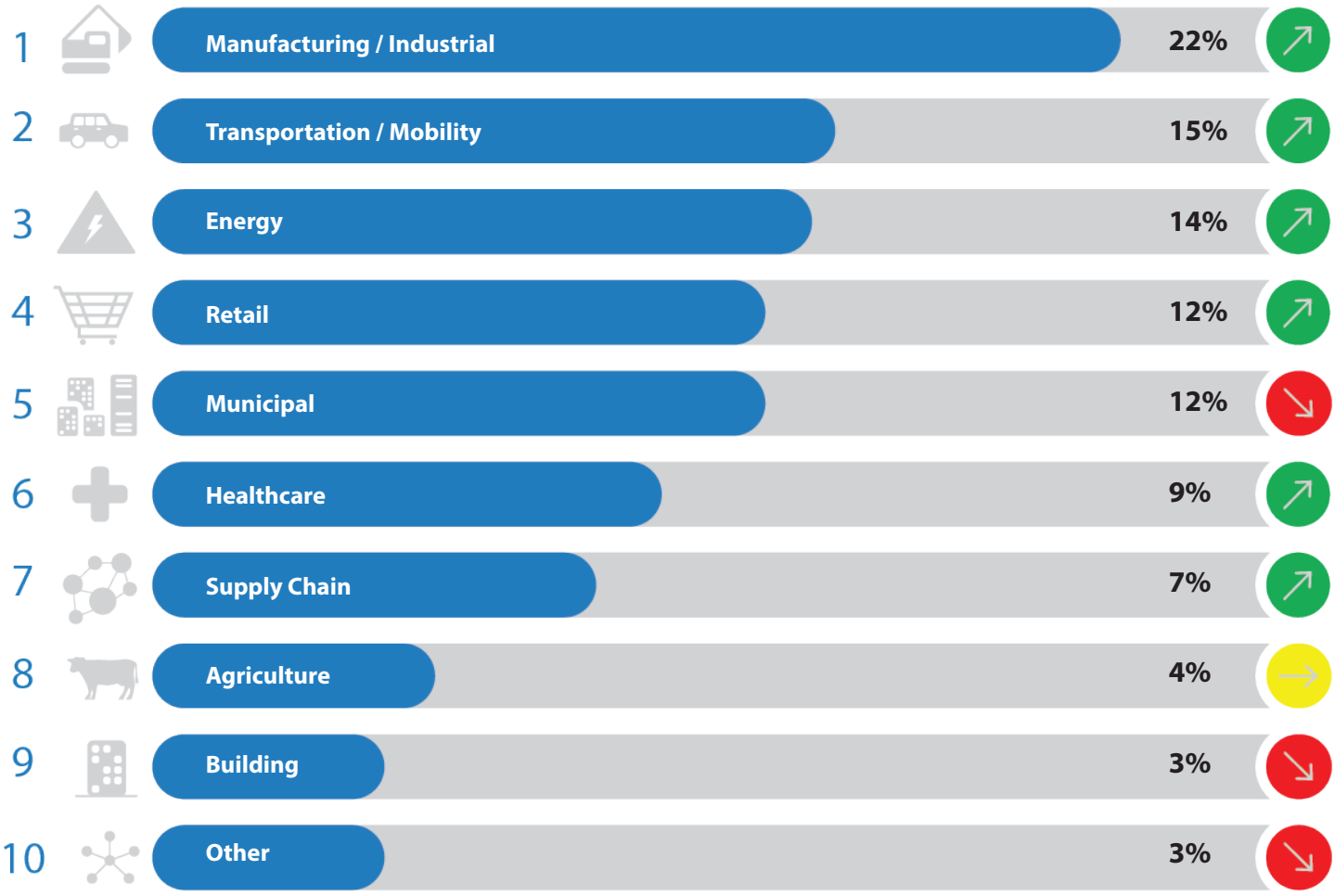
The value of IoT is not only in the raw data capture and sharing mentioned previously, but in the ability for cloud-based software to digitally represent physical assets as "digital twins" (more on this later). This enables OEMs to ensure that the equipment they supply to their customer is operating as intended. The ability to measure historical performance also guides the OEMs to make design changes which can improve reliability and reduce costs. While being able to remotely view a pressure sensor value of 40 PSI may be technically interesting by itself, a more valuable use could be to send an urgent text message to a service manager informing them that "the historical trends of similar equipment, and current sensor value of 40 PSI, indicates that their asset has a 95% chance of failure within the next 1,000 hours of operation. An equipment inspection has been automatically scheduled with the appropriate service team member."

IoT Markets and Business Justification

The market for commercial IoT is booming with manufacturing/industrial as a top segment. This growth is driven by a strong and proven return on investment. Maximizing the returns of an IoT solution involves analysis of the application, feasibility of the technical solution, and a detailed cost-benefit analysis.

Top 10 IoT Application areas 2020

Global Shares of Enterprise IoT Projects



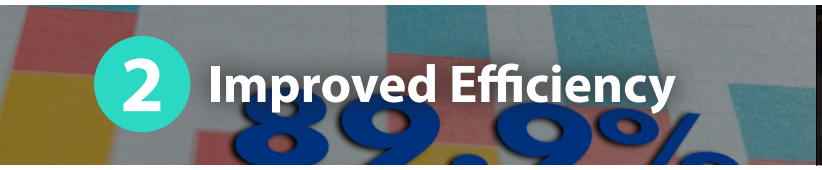
Source: IoT Analytics Research - Chart of Top 10 Commercial IoT Application Areas **N=1,414 projects**

IoT applications have common themes across industries, regardless of the segment. Four core applications are discussed below, and compelling business justifications that leverage IoT technology are presented. These examples can be used separately or in combination to drive deployment in commercial or industrial applications.

1 Predictive Analysis

The most common use case for Industrial IoT (IIoT) systems is to enable improved performance of critical OEM equipment. Physical asset performance analysis, including condition monitoring and failure prediction are the keys to improved outcomes. Today's industry largely operates on a simple model: if the asset is broken then fix it, otherwise check on it periodically. This traditional practice is inefficient. Alternatively, using IoT to predict failures before they occur - while understanding what is needed to prevent a repeat failure - is the better approach. A single failure can often pay for the the IoT system many times over. Furthermore, modern, flexible IoT systems complement legacy systems by identifying failure modes that were never designed to be monitored. IoT is designed to alert OEMs to failures which may be buried within the equipment or inadvertently hidden by the customer or independent service representative. Predicting asset behavior requires knowledge of the equipment, the application and the IoT technology. By working closely with an experienced industrial IoT system designer OEMs can accelerate deployment and gain competitive advantages sooner. Remote access to data about equipment in the field provides huge value to OEMs who are often cut off from the end customer by third-party installers and service providers.

Preddio tip:
When first starting out it is important to begin with a simple approach. We can guarantee that where you start from will be very different from where you ultimately end up. Solutions often fail from being overcomplicated, and you will continuously learn along the way.



2 Improved Efficiency

Improving the energy efficiency of physical assets is a common management objective that can be accomplished using IoT. The combination of rising costs of energy production, environmental concerns, and increased regulations are expanding the need for IoT. Specifically in manufacturing, commercial real estate, and transportation, it is critical to monitor and reduce energy consumption wherever possible. More broadly, OEM designed physical assets consume substantial energy across many applications. Because they are often mechanical or thermal in nature, these assets are prone to degraded operation and failure over time. Using IoT to save energy involves measuring and normalizing ideal performance against environmental conditions. Production results can then be represented digitally as a function of energy consumed, carbon produced, and financial cost versus work performed. While primarily focused on energy savings these efforts will produce additional benefits for manufacturers including higher production quality and extended asset life.

3 Increased Safety

Addressing critical safety issues is another important use case for IoT. In many industries there exist environmental hazards for equipment, people, and surrounding communities. Measurement of high voltage, monitoring of refrigeration temperatures, volatile gas and liquid handling, effluent release of chemicals, nuclear radiation, construction site safety, and unauthorized intrusions are only a few of the areas where IoT is increasingly deployed. These solutions are widely distributed, ruggedized, scalable, and cost effective. IoT solutions are always on, always connected, and remotely accessible. They provide broad, deep, and vigilant coverage of physical assets which is difficult or impossible to achieve through traditional means of monitoring. IoT solutions are also well suited for retrofit applications, augmenting existing systems with additional layers of monitoring and security. This allows for continuous, cost effective improvement of assets over time. In these examples the business case is often driven by the desire to lower or eliminate risk. Improved employee safety, mitigation of environmental impact, and/or compliance with regulatory changes are some of the common benefits. Furthermore, by implementing an IoT solution it may be possible to extend the life expectancy of a facility or critical asset through improved safety and operating conditions.

4 Optimized Productivity

Improving overall equipment effectiveness (OEE) is an important consideration for enterprises and OEMs alike. By leveraging the power of cloud computing and IoT it is possible to deliver exceptional returns. Industry 4.0, powered by IoT, broadly represents many emerging methods all focused on improving productivity and reliability. Productivity use cases can deliver the highest returns on investment. While these applications are complex to implement, an experienced IoT designer can help OEMs prioritize and design practical starting solutions.

Preddio tip:
Don't sink your IoT program before it takes off by focusing on applications with cloudy (pun intended!) business justifications; start simple and leverage production data that is readily available.

The Need to be "Connected"

Consumer IoT systems are typically connected to the Internet via the homeowners WiFi network. Setup is simple using a free app and an onboarding process where WiFi credentials are shared with the IoT device. In these environments, if a bad actor were to gain access to the homeowners network it would be bad, but not catastrophic. By contrast in industrial and commercial settings there is a greater need for security, access control, and user authentication. This is for good reason, but usually the answer is not to simply beef up the security and complexity of the IoT device before granting access to the enterprise network. Rather, by distancing the IoT solution from the existing enterprise network you can limit exposure, increase redundancy, and decrease implementation cost.

Simplicity is key to IoT adoption and most importantly, these solutions are acceptable to many enterprise IT organizations as they are separate from existing enterprise networks.

Preddio tip:

Compare a cost-benefit analysis for getting enterprise approval, site-wide integration, and updated user training for a massive system upgrade vs. investing in a stand-alone highly secure solution that can often be installed in hours without any approvals needed.

While generally easier than connecting equipment directly to an enterprise network the design and deployment of IoT solutions do require detailed planning. Below are a few principles that if followed will lead to an effective solution:

Best in class cyber security is always a core requirement;

Reliance on existing enterprise connectivity should be minimized;

Data should be available for authorized users anywhere in the world via secure Internet-based applications;

Installation and operating costs should be lower than traditional enterprise networks; and

Data flow should never be impeded by changes in the enterprise network.

Only a few years ago, these IoT solution requirements would have been extremely hard to achieve due to technology and infrastructure limitations. Fortunately with a recent surge in large and small companies contributing to IoT infrastructure, there are a number of wireless communication methods which can be used to satisfy the above-referenced objectives. The table below compares some of the various ways to wirelessly connect IoT solutions to the Internet without relying on traditional enterprise networks.

Technology	Power	Distance	Data Rate	Cost	Native App	Gateway Router
Bluetooth®	• • •	• •	• •	• • •	Yes	No
Zigbee®	• • •	• •	•	• •	No	Yes
LoRa®	• • •	• • •	•	• •	No	Yes
WiFi®	• •	• •	• • •	• •	Yes	Yes
Cellular	•	• • •	• • •	•	Yes	No

(note: • • • is ideal, • • less ideal, and • not ideal)

Bluetooth is a great technology because it is found in almost every smart phone or tablet. Many apps and systems use Bluetooth to easily and securely connect directly to an IoT device. For many applications and use cases this is the most straight forward approach (when implemented correctly) to instantly view data from an IoT device. However, Bluetooth is not directly accessible via the internet, meaning that some sort of gateway (more on this later) is needed.

Zigbee is a low power, scalable, mesh capable protocol that is commonly used for lighting and building controls, but is limited by low data rates and is plagued by silicon vendors interpreting the standards in their own best interest. ZigBee is also not accessible directly via the internet.

LoRa is gaining popularity as a low power, long distance technology but also has extremely low data rates, and like Bluetooth/Zigbee needs a gateway to reach the Internet.

WiFi is ubiquitous and a good choice for IoT devices that are allowed into a home network but has added complexities and deployment costs which make it unsuitable for enterprise environments.

Preddio tip:
Don't get into an argument about the "best" protocol to use, there are often trade-offs to consider. Let the application requirements determine the best technology to use, not the reverse. Also be wary of solution providers who are overly dependant on proprietary standards that can be slow to innovate and react to market needs. Finally recognize that cyber secrity is always a requirement reguardless of the particular standard you select.

Cellular technologies have seen tremendous growth in the past few years, due to the advancement of 3G/4G/5G and global coverage networks. With cellular, IoT devices can have direct and secure access to the cloud bypassing the need for integration into existing IT infrastructures. Depending on operating budgets to account for data fees, and the potential need for access to power, cellular is becoming a widely adopted technology for IoT.

There are certainly experts who will debate these viewpoints; however the important takeaway is that any of these technologies can be surrounded with supplemental systems to accomplish your business goals. Just be careful when a solution provider leads first with their existing approach, before fully understanding your specific challenges. If they are a hammer, everything will look like a nail to them.

In order to understand and predict what the future might hold for wireless technology adoption, let's look back into history. During the 1990's the deployment of Ethernet for factory automation became popular and was in direct opposition to the incumbent five or six existing proprietary industrial standards (Interbus, Profibus, Modbus Plus, MPA, Echelon, DeviceNet, etc…). By leveraging the openness, relative low cost performance and scale of the commercial success, Ethernet also became the standard for industrial applications (even displacing some of the previous "standards"). Using history as a guide it is likely that IoT will follow a similar convergence towards cellular.

Though by no means dominant today, 5G for IoT applications is growing rapidly, especially when compared to the other wireless alternatives. Cellular is a proven commodity, it is highly secure, can run independently from the enterprise network, and is pervasive. As mobile carriers (AT&T, Verizon, T-Mobile, etc...) are increasingly offering IoT data plans designed for mass adoption, a new standard for Industrial IoT communications is emerging based on 5G. We can expect that this trend will continue, and currently more expensive than alternatives, further commoditization should dramatically decrease the cost of cellular over the next several years.

Gateways – Connecting the "I" to the "oT"

Gateways are used in many IoT installations today. The main purpose of an IoT focused gateway is to provide remote access to sensors that need a persistent connection to the Internet. These sensors are typically numerous in quantity, have limited battery life, and do not contain enough computing power to operate on their own. Creating a direct Internet connection for each sensor can be too expensive or complex, and gateways are a common solution. Aside from connecting on site devices to the Internet, gateways can play an even more important role in the day-to-day interactions of devices within an enterprise facility.

Correctly designed and installed gateways can make all the difference between success and catastrophic failure for many business initiatives, both in terms of cost but also performance. Sometimes even life or death. Think about it, not all applications have the luxury to wait for data to be sent to the cloud, processed, and instructions sent back. What happens if power is lost, a cell tower goes down, or someone makes a mistake at a data center? This is where the "edge" comes in, and gateways can play a critical role in mitigating disaster.

What do we mean by "the edge" and why does it matter? In some cases, sensor information is processed and acted upon on site without needing a persistent connection to the Internet. This is incredibly important when there are massive amounts of data that should not or cannot be sent to the cloud, or when an immediate response is needed (think life or death safety situations). In these applications, gateways that sit at the "edge" of the network can have the intelligence to make decisions locally when a connection to the Internet is not available or needed.

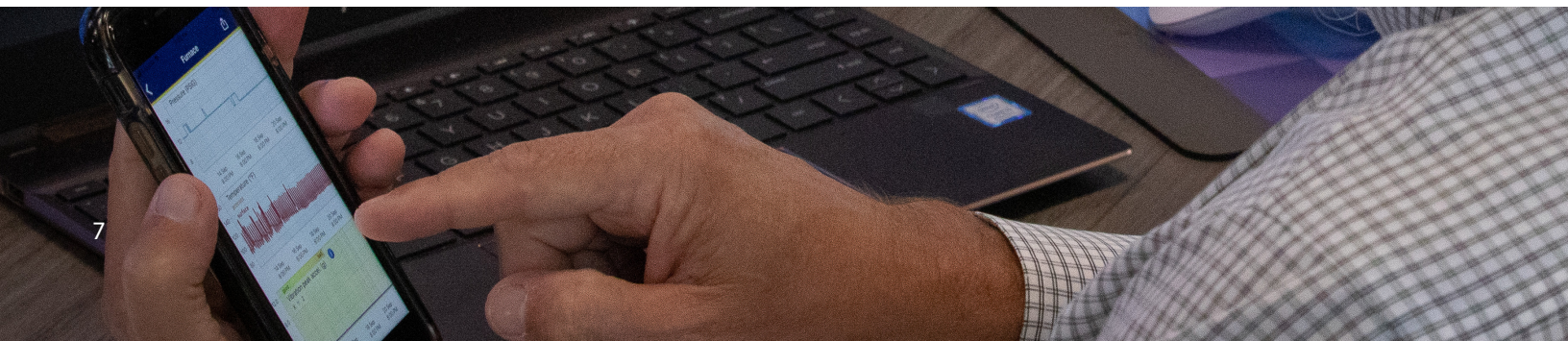
Another requirement to consider when designing or selecting a gateway is how fast the data needs to be updated. This depends on what "real time" means to the application and what a tolerable delay is. The data update frequency from the sensor to the cloud can range from days to only a few milliseconds. Costs are directly linked to the amount of data, and frequency that it is uploaded to the Internet. This can affect the profitability or feasibility of an IoT platform. The table below gives a broad overview of common applications, latency (tolerable delays), how often information is transmitted (update frequency), and how much data is processed (bandwidth):

Gateway Performance Guidelines

Application	Tolerable Delay	Update Frequency	Bandwidth	Good for IoT
Video Surveillance	Seconds	Real Time	High	Yes
Remote Diagnostics	Seconds	On Demand	High	Yes
Interlocking and Machine Monitoring	Milliseconds	Milliseconds	Low	No
Closed Loop Process Monitoring	Seconds	Seconds	Low	No
Machine/Process Monitoring	Seconds	Seconds	Low	No
Equipment Condition Monitoring	30 min	10 min	Low	Yes
Air Quality Monitoring	5 min	30 min	Low	Yes
Energy Management	30 min	30 min	Low	Yes

In summary,

gateways have the capability to translate and collect information from numerous types of sensors, selectively deciding what information to send to the cloud and when to send it. This level of intelligence and sophistication is usually not found, or needed, directly in each sensor. It would be redundant, incredibly expensive, and difficult to maintain for operators. Successful IoT implementations provide the right balance of sensor complexity, gateways, and intelligent decision-making capabilities when time is of the essence or the Internet is not available.

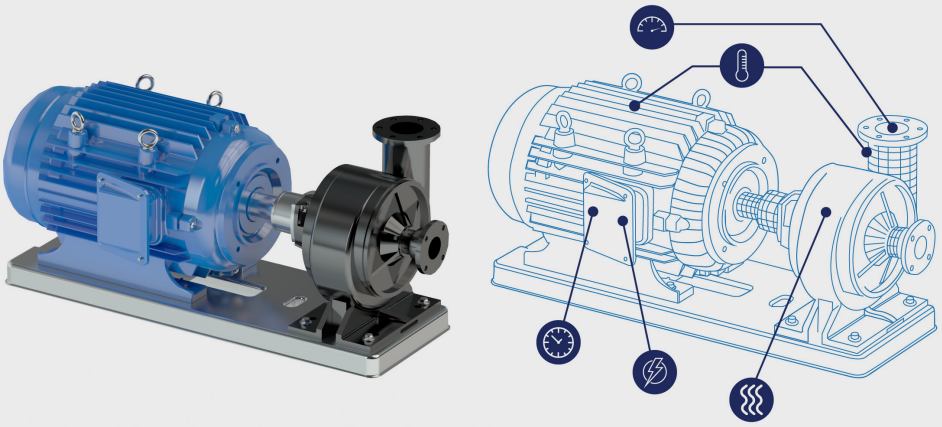


Leverage Digital Twins

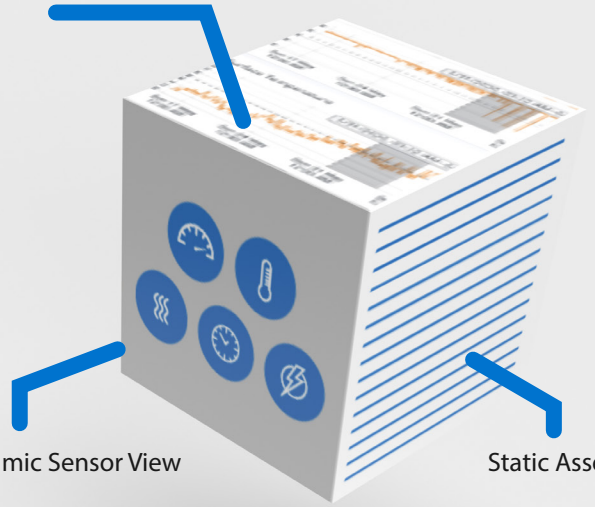
An up-and-coming aspect of IoT is the concept of Digital Twins (digital replicas of physical assets). Successful IoT programs deploy digital twin concepts as a way to make sense of complex data. Data without relevant context is redundant to existing legacy systems, expensive, and provides limited value. Alternatively, multi-dimensional data represented successfully by a digital twin adds tremendous value to enterprises. This digital representation can provide powerful insights into how physical assets are operating now (the present), have operated (past history), could be operated (immediate recommendations), and should be operated (long-term reliability).

Compared to traditional industrial control systems, IoT is relatively young, and the digital twin concept is still maturing. However, there are enough successful examples operating in the world that these principles cannot be ignored.

IoT solutions have leveraged digital twins in a variety of ways; from simple (but eye-catching!) robotic arm images with sensor data superimposed, to extremely complicated algorithms and visualizations that require a PhD to comprehend.



Performance View



Dynamic Sensor View

Static Asset View

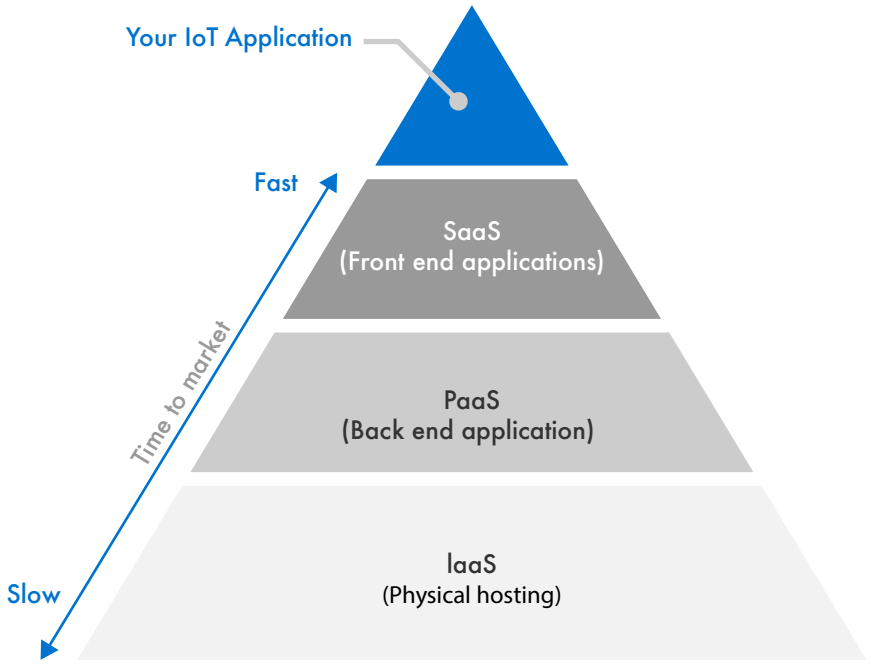
It may help to think of a digital twin as a 3-dimensional object,

an expandable framework of metadata, key indicators, and attributes, which are constantly updated. At a minimum, it contains any combination of dynamic (sensor) data, static (asset) data, and performance (analytical) data, all managed and represented as a single entity. Without going too far into the weeds, below are some high-level use cases:

- **Comparison of similar objects** – the ability to compare all technical attributes and operational insights from similar pieces of equipment, operating in different industries, trended over time
- **Dashboards** – the ability to have an unlimited number of unique digital viewpoints without the need to constantly rebuild databases or create new frameworks
- **Predictive data** – the ability to trend and compare assets across any time period, learning from previous events to predict future behaviors
- **Ideal operations** – the ability to monitor the behavior of physical assets vs. the ideal operational parameters they were designed for.
- **Systematic operations** - the ability to view multiple assets working together to achieve a shared purpose

Implementation of Cloud Applications

Perhaps the most important and customer-facing aspect of IoT is the cloud application, a web-based interface to all of the benefits that IoT brings. As technology has matured, modern software has increasingly become packaged as recurring services rather than one-time purchases. IoT has benefited from this phenomenon through the abstraction and consolidation of the most commonly needed IT services into three distinct platform layers. These layers are needed to support specific end-user applications. OEM manufacturers and solution providers alike can choose to build none, all, or some of each layer. Deciding to build or partner requires careful consideration of time to market needs, existing technical staff, required market differentiation, and investment capacity. Below is a high level summary of the three platform layers critical to supporting IoT applications:



Infrastructure as a Service (IaaS):

This is the lowest possible level of cloud "infrastructure," essentially the physical computing hardware which the Internet is built upon. Think Amazon Web Services, Google Cloud, Microsoft Azure, data centers, etc. Billions of investment dollars have gone into this market already. We recommend that your application be built upon at least one of these "name brand" players in the market (and certainly not with a company you or your customers have never heard of).

Platform as a Service (PaaS)

On top of the infrastructure sits your application "platform." Think of this as operating all of the administrative services needed for your application to be managed, secured, and distributed to users. These services are usually generic in nature, not tailored to specific industries or use cases, but horizontally scalable and mission critical to successful cloud operations. However, trying to build and maintain these services on your own requires a large operations staff and continuous investment into upgrades and improvements.

Software as a Service (Saas):

Just below your end application sits the most configurable and unique set of services that are developed for IoT applications. This layer contains all of the specific requirements for your end-users. The look and feel, user experience, and unique features that differentiate you in the market are all enabled by this layer. Because the SaaS layer is so close to the equipment, sensor, and application needs, the large cloud providers will not have an "out of the box" solution. Unless you have a staff of developers, you will need to partner with an expert to help build your solution.

As you can see, there has already been a tremendous amount of investment and effort from great companies put into the above services. Building everything on your own is no longer necessary and choosing the right partners to work with can eliminate risk while speeding up market entry.

Preddio tip:

Be wary of solution partners who try to do too much on their own (for instance we have strategically chosen to focus on the top level SaaS and application layers, partnering with experts for the lower PaaS and IaaS levels).

SaaS – A Closer Look

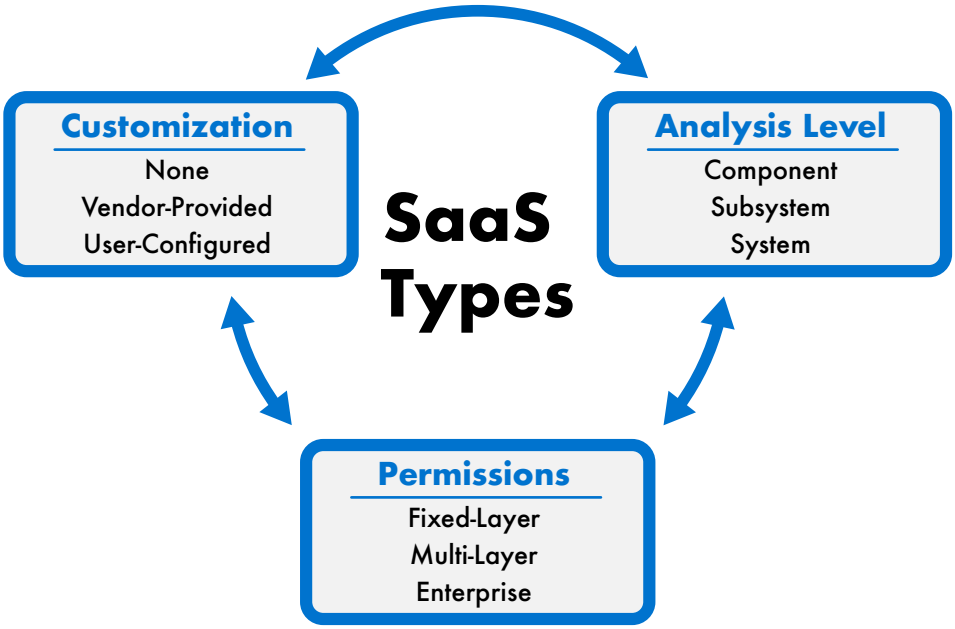
Within SaaS platforms there are many types of applications and requisite life cycles to be aware of. From design through deployment to long term operation and maintenance, you are engaging in a long-term commitment. Technology innovation is not static, and there will always be changes in the underlying platform requirements, "bugs", or requests for new features at your doorstep. Furthermore, deciding what types of SaaS applications to integrate is not an easy process. Likely your IoT solution will require the combination and customization of many. Picking a partner (or partners) who can effectively translate your requirements into an IoT application will make or break your program, and ideally allow you to focus on your core business without needing to worry about the underlying mechanics.

Here are a few examples of common SaaS topics and underlying decisions to be aware of:

Customization – discuss how you will handle requests for user interface changes and if you or your customers will be able to implement them yourself or need to rely on the vendor

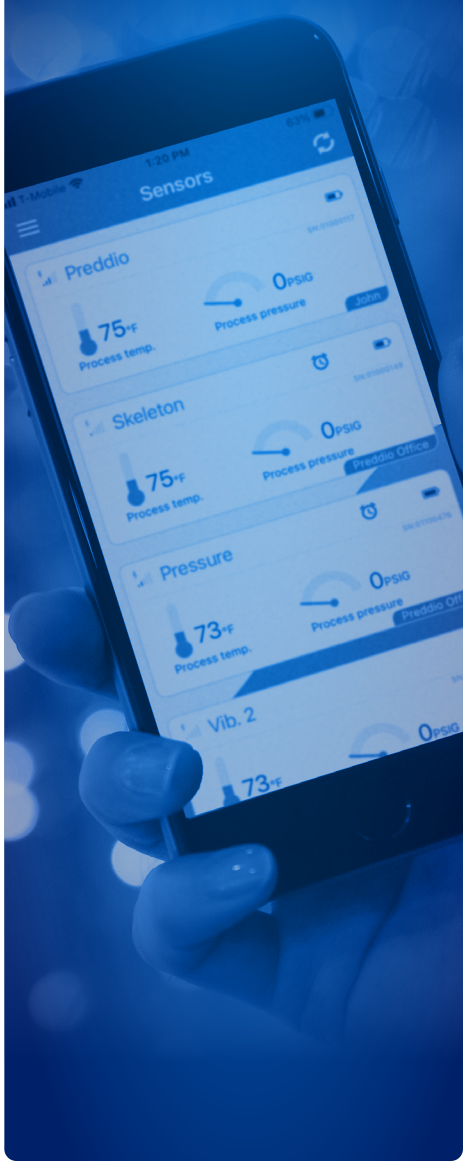
Hierarchy – define the digital structure for your assets (locations, groups, systems, sub-systems, components, to name a few)

Permissions – distinguish between different classes of users, administrators, and operators



Preddio tip:

When partnering with a platform company, be sure to evaluate their health as a business, track record, development practices, staff capabilities, security practices, and ability to scale to your needs. If in doubt, try a pilot project with them for a minimum of three months.



Starting your own IoT journey

Like most new technologies and "shiny objects" that seem compelling, you should always do your due diligence and test drive when possible. In the early years of IoT, many engagements failed because of a lack of experience, clear requirements, or maintenance commitment. Non-electronics focused OEMs without prior IoT experience should think through the "what" and "why" of the solution to make sure it makes sense. Think about both carefully, and consider getting answers to the questions below before you get started. Whether you are doing your own development, or partnering with a solutions provider like Preddio Technologies, at a minimum your organization needs to answer the following questions:

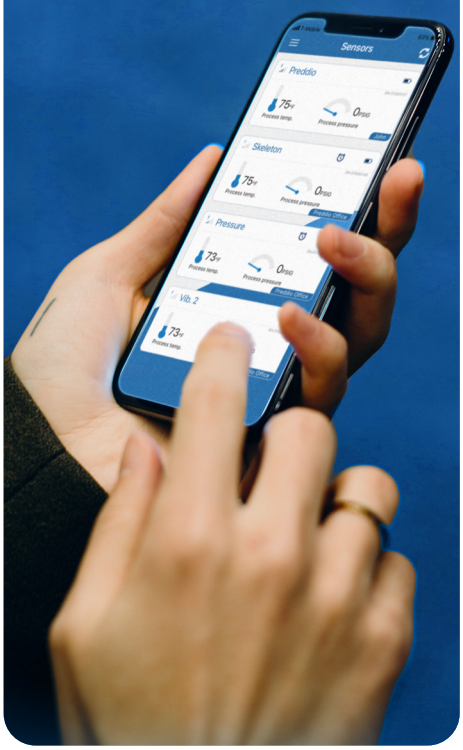
Requirement Questions (The What)

- What solution is currently in place, do we need to install a new or different one?
- What locations are to be monitored, are they far apart or close together?
- What are we looking to discover, enable or prevent from happening?
- What needs to be monitored and how many sensors do we need?
- What types of information are we looking to trend over time?
- What types of sensors do we need (i.e., industrial, commercial or residential)?

Business Questions (The Why)

- Why do our customers care about the solution; do they benefit from cost savings, increased reliability, risk mitigation, improved productivity or safety improvements?
- Why can we justify the value of the solution to our customers; will we lease the solution, charge a fixed fee, allow them to resell the offering downstream?
- Why do we deserve to compete with the existing solutions in the market; will we commit to a cycle of continuous improvement and competitive evaluation?
- Why will our dealers and channel partners embrace this solution?
- Why can the IoT program be justified; what KPIs need to be met in order to be successful?
- Why are we capable of running and maintaining the IoT solution after we develop it; are we able to shift our mindset, service and sales processes?

"IoT" Technology isn't new, and isn't a reason to reinvent the wheel by making it square.



Preddio Technologies – Your IoT Solutions Developer

Want to learn more?

Contact Us

We would be happy to explore mutual possibilities.

Sales@preddiotech.com

www.preddiotech.com

At Preddio Technologies, our approach to IoT implementation begins first with obtaining a deep understanding of your opportunities and goals. Our clients cannot afford to solve problems that don't exist, and we are not afraid to challenge their assumptions. Only after the positioning statements are solid do we even begin to recommend a technical approach. Our in-house development team is comprised of multidisciplined electrical, mechanical, and software engineers with decades of combined experience. Rather than designing new systems from scratch which are costly and time intensive, we draw from a library of Powered by Preddio™ building blocks. Fine-tuned to the specific application needs, we will collaborate with you to provide sustainable and monetizable solutions for your business. With over 30 million (and counting) data points under management in our cloud, we know IoT.

At a high level, our customers turn to us to provide:

- **Analytics –** while keeping it simple, we translate massive quantities of raw sensor data into meaningful dashboards and delightful user experiences
- **Predictability –** we love difficult problems and understand the urgent needs of our customers to **predict** unforeseen events, **prevent** them from happening, and **prepare** for the future
- **Reliability –** we spend our nights and weekends worrying about server uptimes, security, and data authenticity so that our customers don't have to

We realize that you have many choices when it comes to IoT solution partners. Technology approach, feature set, and costs can all be manipulated to look good on paper – but this does not matter. What matters most is that you find a partner you can trust, who shares mutual goals, and who is committed to innovation and excellence. We don't do what we do because we have to; we do what we do ***because we love to do it.***

Thank you for reading!

Sincerely,
Your Preddio Technologies IoT Team