BostonDynamics

WHITEPAPER

Getting Started with Industrial IoT

What to consider when deploying Internet of Things (IoT) solutions, and when to adopt a more dynamic approach.

Contents

3...... IoT momentum

4.......The fundamentals of an IoT deployment

6...... Communication and connectivity challenges

7.......The move to dynamic sensing as a solution

8.................The fixed approach

9.................The dynamic approach

10...............A pre-deployment IoT checklist

11......Choosing the right combination for your IoT environment

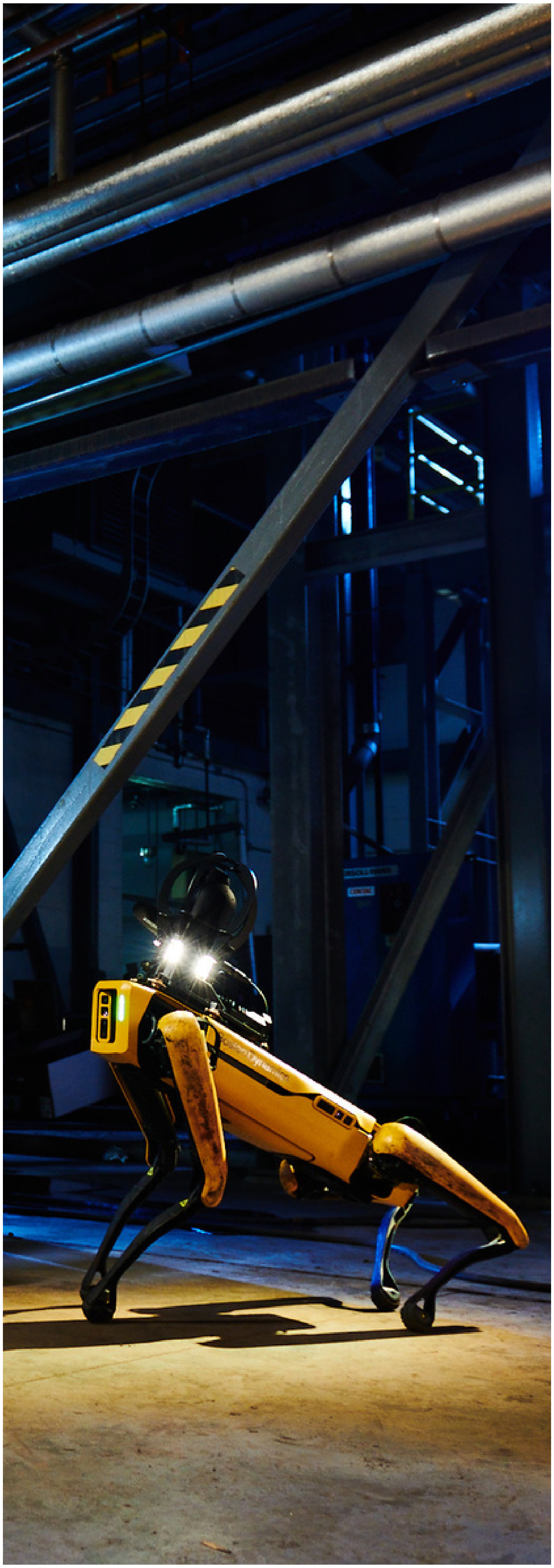
IoT momentum

With large capital expenses invested in their production assets, manufacturers need those assets working at capacity. Every hour of downtime is expensive—unplanned downtime is even more so.

One of the tenets of an effective Industry 4.0 strategy is to keep production running by analyzing real-time data at scale to predict and prevent issues that otherwise lead to downtime. This near-continuous production relies on machine-machine communication through the Internet of Things (IoT). As part of an IoT ecosystem, sensors throughout a manufacturing facility capture and communicate necessary information for analysis. At the backend of the IoT ecosystem are machine learning models trained to recognize normal (or abnormal) machine behavior and deliver actionable insights accordingly.

IoT deployment, a key part of digital transformation, is not for manufacturing alone. Any industry which works with machines, equipment, or other assets can use IoT to realize efficiencies; as a result, this technology is on a meteoric growth curve. By 2025, there will be an impressive 27 billion IoT installations around the world, according to IoT Analytics.

So what's really under the hood when we talk about IoT? And why does it matter if an IoT deployment uses fixed or dynamic sensors?



The fundamentals of an IoT deployment

IoT is about machines talking to each other in order to automate processes or make them more efficient. This approach requires several different technologies, beyond the sensor itself, working in concert to turn raw data into meaningful insights.

An IoT ecosystem usually includes:

1. The IoT Device

An IoT-enabled device starts with a sensor that can measure whatever the relevant parameter is. Sensors might include thermal cameras to find hotspots, acoustic imagers to detect air leaks, hygrometers to measure humidity —or any other kind of sensing and data capture device.

The IoT device will also carry a microprocessor for simple computations, a communication port to relay information, and a power supply.

Components of an IoT System

1. **IoT Device**
   A device that can sense specific parameters, collect data, and sometimes perform basic actions in response to inputs. (For example, turning a lever off if the water level in a tank exceeds a certain level.)

2. **Communication System**
   Communication protocols and infrastructure relay information from individual devices to data aggregators and distributors.

3. **Analysis Software**
   Once the data from each sensor is aggregated, software analyzes it for insights, which can be communicated back to relevant systems, devices, or operators.

2. Communication System

An IoT strategy needs a path for data to move from the device where it's collected, to a person who can act on these insights. This requires reliable communications infrastructure. The system might include gateways, which function as data aggregators. They collect information from neighboring IoT devices, prescreen them and add encryption if necessary, before routing on to the internet for processing by a downstream analytics tool.

Servers corral all information coming in from the gateways and route data for computing. Some IoT applications, like vibration monitoring on pumps, motors, and compressors, do not require immediate action, so information gathered can be sent off to be processed through cloud computing. In other instances, such as detecting hazardous gases or other threats to people, the speed of response to incoming IoT data matters. In such cases, computing will need to be carried out close to the source of data, and enterprises will usually prefer edge computing.

Popular connectivity methods include:

WiFi

Uses familiar Internet protocols such as Transmission Control Protocol/Internet Protocol (TCP/IP) to relay data. It is expensive, demands heavy power requirements of the IoT device, and is not feasible for large-scale deployments.

Low Power Wide Area Network (LPWAN)

Well-suited for IoT devices that transmit data infrequently—data is not constantly livestreamed—and where low power consumption is critical. Large-scale IoT deployments where latency is not a factor can benefit from LPWAN-delivered connectivity.

Bluetooth and BLE

Tried and tested options for basic IoT devices, they are limited in their range however, and are not very feasible for long-range applications.

Zigbee and Z-Wave

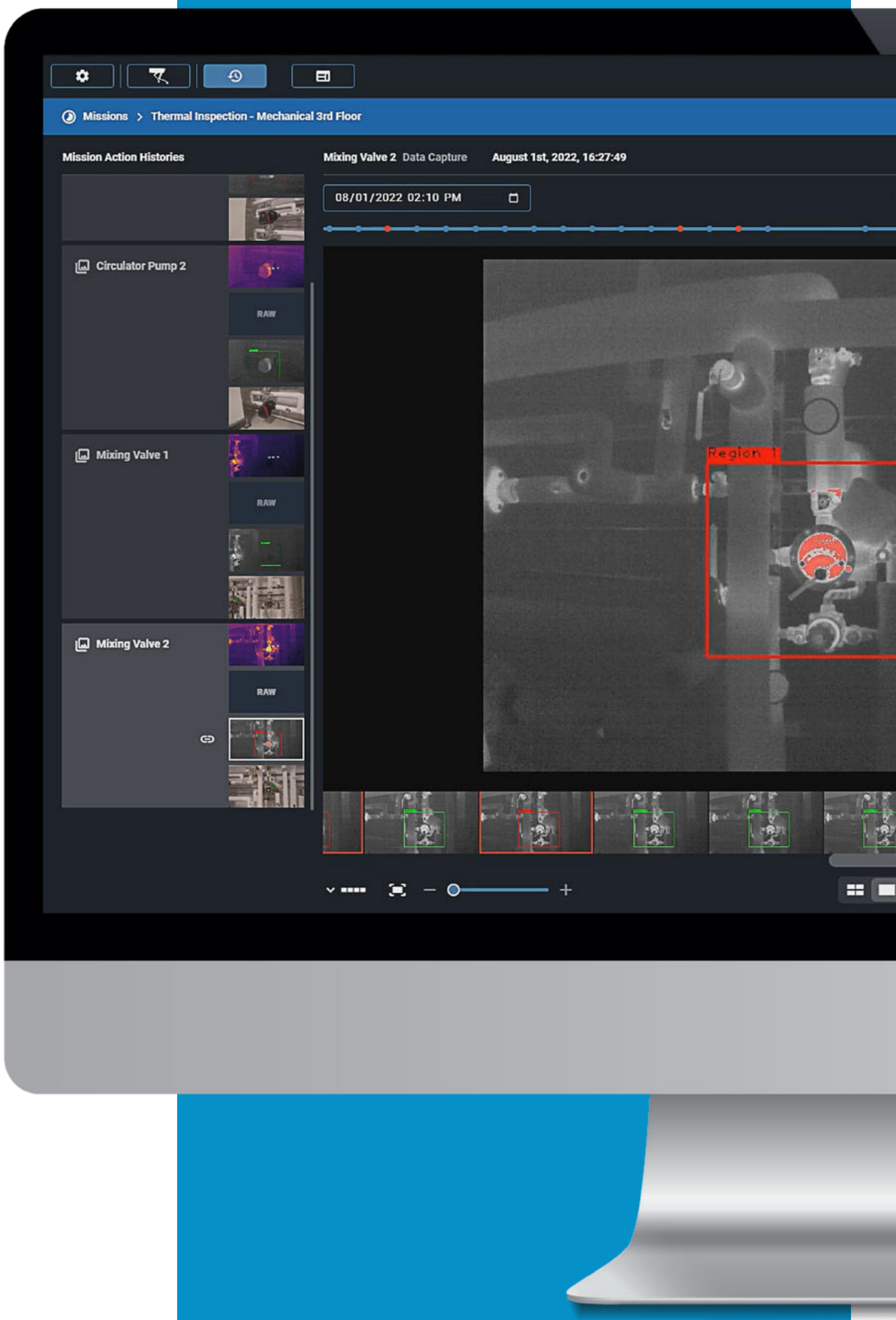
Made for low-power, low-bandwidth delivery and frequently used to connect smart devices within a small geographical area such as home or office. Since neither supports internet communication protocol, data has to route through an intermediary gateway before it can be used.

Cellular Networks

Enable IoT devices to communicate over larger distances, especially with specific protocols like Cat-M and NB-IoT. Adoption of 5G brings a lot of promise for deployment of high-data sensors like video cameras, but costs of complementary architecture can be high.

3. Analysis Component

Finally, an IoT deployment needs software that analyzes the data stream and sounds the alarm if critical thresholds are met. This typically includes a platform for visualizing results and controlling a fleet of IoT devices. In advanced cases, machine learning models do the heavy lifting, learning from new and historic data. Operators can review the data outputs in SCADA systems or Enterprise Asset Management (EAM) solutions, and receive automated alerts or work orders based on the analysis.



Communication and connectivity challenges

Machine-machine communication is arguably the backbone of IoT technology. It is also the most complex and, frequently, one of the most significant cost contributors to an IoT deployment.

IoT communication must solve two basic challenges:

- How to make data from different machines talk to each other
- How to relay this data from all devices on to the internet

If the internet connectivity of choice does not homogenize communication formats from different device manufacturers, then application protocols come to the rescue. MQTT and CoAP are popular protocols which can scrub the data to standardize communications.

The more daunting problem in IoT deployments is getting all that data efficiently transferred to systems where it can be put use. The options will depend on, among other factors, the vastness of the IoT deployment, which will determine the amount of data flow, and the frequency of data collection.

Figuring out the right technology architecture for specific deployments is one of the biggest challenges for enterprises.

For one thing, the options for internet connectivity vary and costs increase depending on the amount of data enterprises want transmitted—and when. Small packets of data relayed intermittently, such as temperature readings, will likely cost less than continuous feeds of video data.

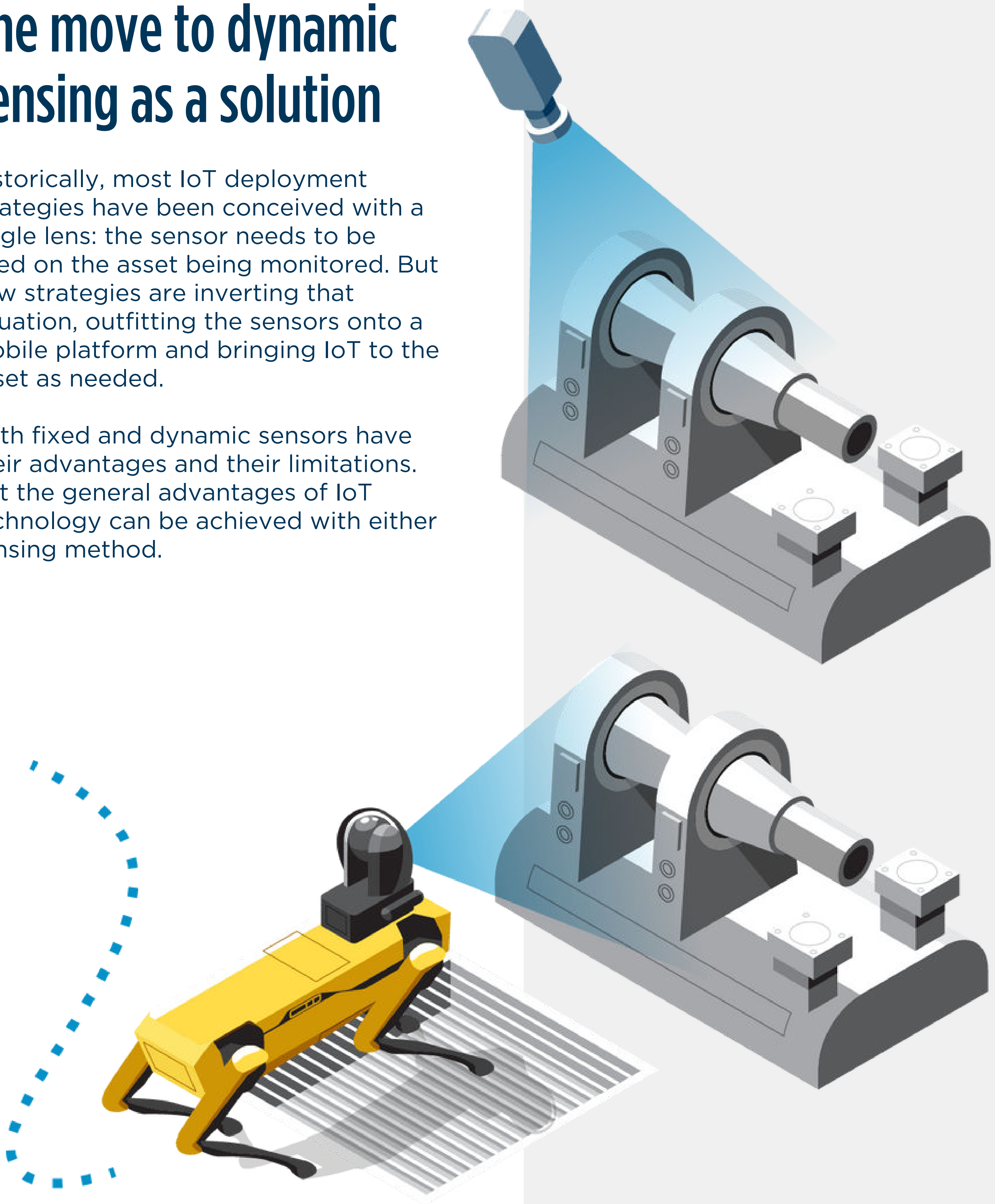
Comprehensive, custom IoT solutions can vary widely in terms of both complexity and cost, from $50,000 minimum viable products to million dollar full-scale enterprise applications. In fact, technical complexity and budget constraints are the two biggest blockers for companies who want to utilize IoT, according to research from Microsoft.

While 4G LTE and 5G are lauded as the platforms for IoT expansion, the costs of servicing remote areas continues to be a concern. Temporary networks for remote locations, or areas where connectivity can be spotty, are an option, but they can add on to IoT deployment costs. They also might be overkill if enterprises haven't fully mapped their IoT strategies and are looking for stopgap pilots to create an initial plan.

The move to dynamic sensing as a solution

Historically, most IoT deployment strategies have been conceived with a single lens: the sensor needs to be fixed on the asset being monitored. But new strategies are inverting that equation, outfitting the sensors onto a mobile platform and bringing IoT to the asset as needed.

Both fixed and dynamic sensors have their advantages and their limitations. But the general advantages of IoT technology can be achieved with either sensing method.

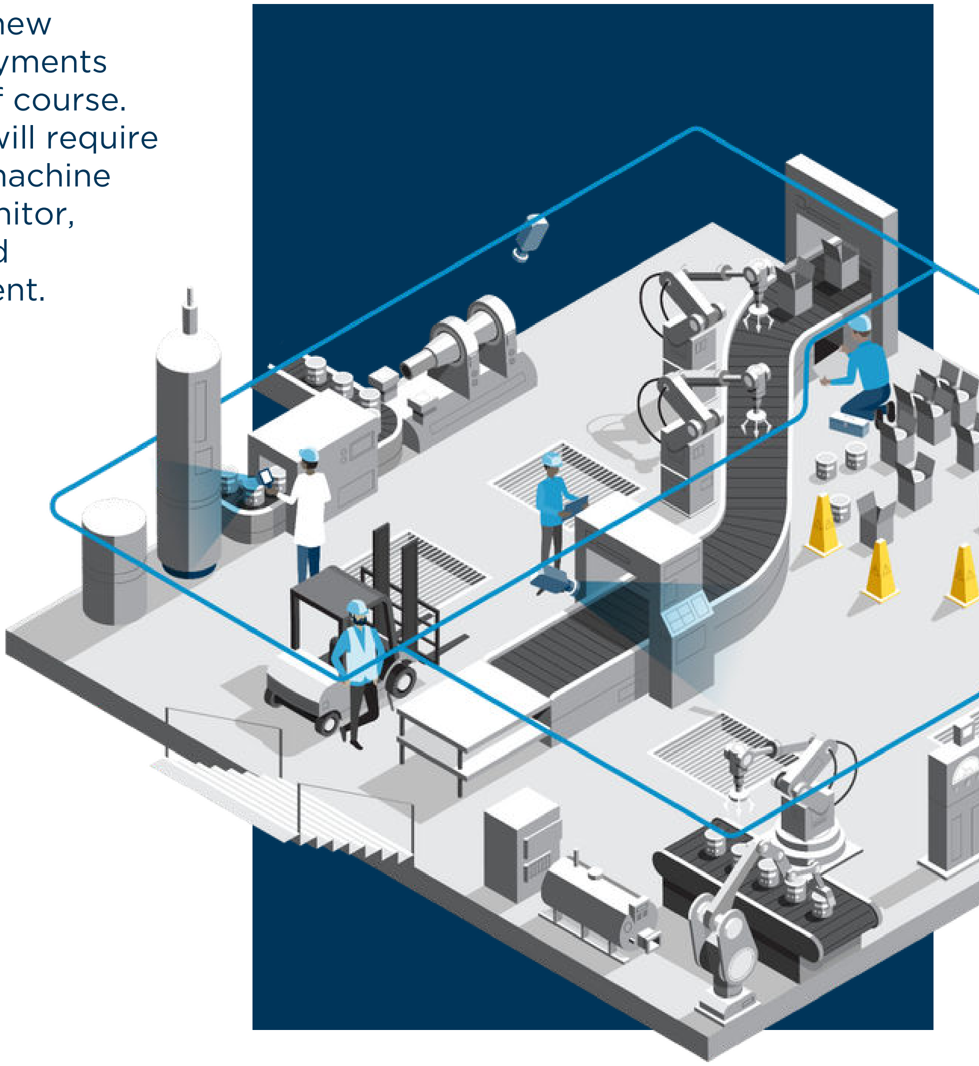


The Fixed Approach

Fixed sensor IoT deployments involve stationary sensors installed on or near the devices that need to be monitored. At predetermined intervals or even continuously, data from these devices relays on through a gateway with an established connectivity method for processing. While fixed sensors offer a low touch approach to IoT day-to-day, factors like calibration and battery limitations can impact maintenance and upkeep.

At greenfield facilities and on new equipment these sensor deployments may be included as a matter of course. However, in most cases, sites will require a unique installation for each machine and data type you want to monitor, which can quickly add cost and complexity to an IoT deployment.

Retrofitting older equipment may also lead to data gaps when managers cherry pick the machines that qualify for this level of monitoring. Technology upgrades are also difficult and expensive to maintain, especially at facilities requiring more extensive retrofits. If a facility's equipment changes, existing fixed IoT sensors can become unusable and obsolete.



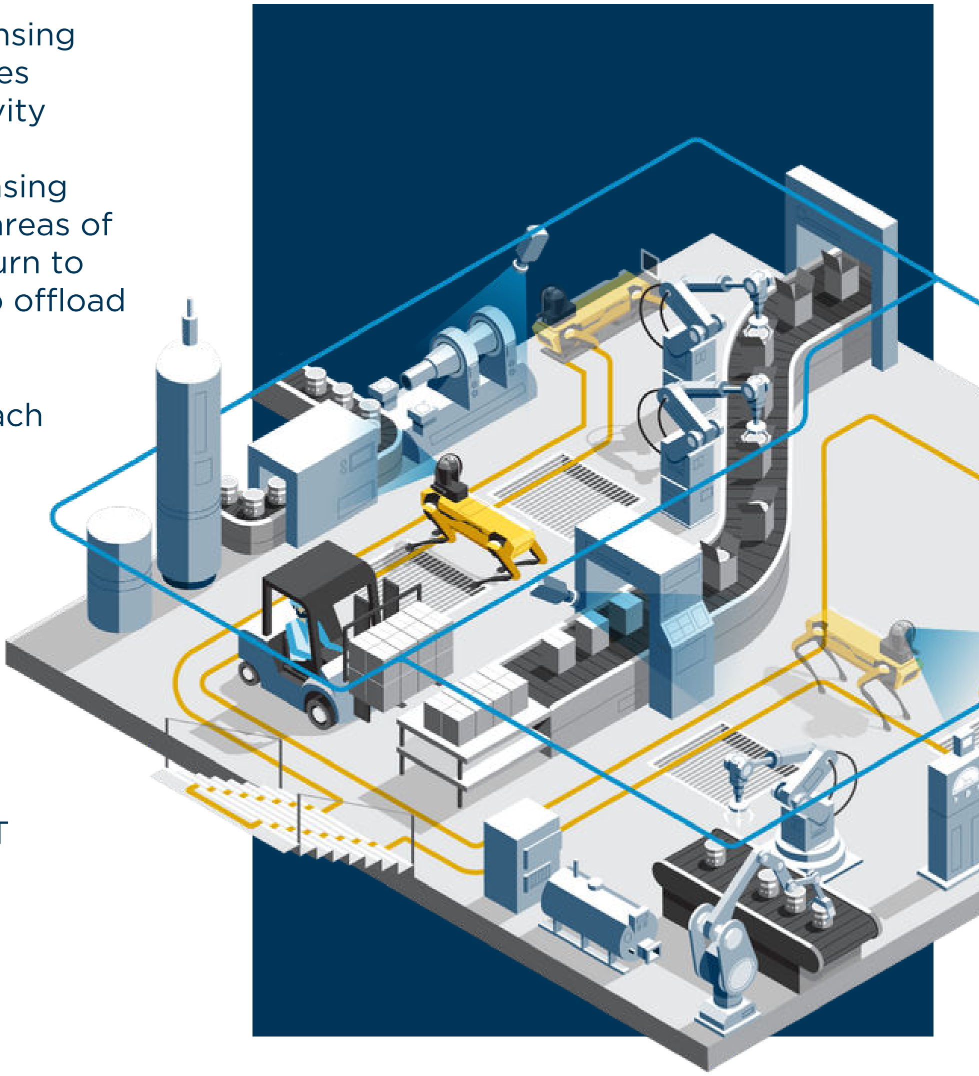
The Dynamic Approach

Dynamic sensing brings the sensors to the machines. A mobile robot can be outfitted with the appropriate sensors and dispatched on site—a few sets of sensors on a single robot can cover an entire facility. Dynamic sensing is agile enough to accommodate changes in data demand. Enterprises aren't limited by fixed data from fixed sensors; they can be selective in mixing and matching their inputs based on what they are looking to measure.

Equally important, dynamic sensing reduces the capital expenditures involved in outfitting connectivity infrastructure for entire IoT deployments. The dynamic sensing platform can measure data in areas of low or no connectivity and return to areas with high-connectivity to offload collected data.

Additionally, a dynamic approach can be easily adapted as your sensing needs evolve, instead of reworking fixed installations to accommodate changes. As a result, dynamic sensing lowers the barriers for IoT deployment and can be effectively used for IoT solutions in brownfield facilities that would require retrofitting to support fixed IoT implementations.

With that in mind, dynamic sensing isn't an always-on solution the way fixed sensors are—the robot needs to be dispatched regularly to gather consistent data and catch key warning signs. The ability to reuse a few sets of sensors throughout a facility is one of the strengths of dynamic sensing, but it requires a strategic plan for how to deploy your robotic fleet to ensure the desired level of coverage.



A checklist before IoT deployment

Given the various parameters involved in successful implementation of IoT, it's helpful to run through a set of factors to consider before customizing the technology for a given enterprise's needs.

1. **Cost**
What will capital and ongoing operating expenses be? This means looking beyond the direct costs of sensors to also include the costs of connectivity infrastructure and increased demands on IT.

2. **Data**
Working backward from key performance indicators (KPIs), enterprises need to figure out which data to measure and from which fleet of machines. These requirements can change so they need to be a periodic exercise.

3. **Integration between IT and OT**
Companies will have to work out the logistics of how to use data they receive from OT deployments (Operational Technology) and how to integrate it into their existing IT infrastructures for maximum benefits. Understanding where and how quickly the insights will be acted on will also be key in deploying a mix of edge and cloud computing.

4. **Fixed or dynamic sensors**
These will depend on the costs enterprises are looking to control as well as the reasons for data gathering in the first place. Routine inspections can be outsourced to dynamic sensing platforms.

5. **Connectivity**
The ways in which the IoT data travels for analysis vary, so picking one or a combination of them depends on the geographical range enterprises are looking to cover, the extent of deployment, and connectivity and messaging costs.

Choosing the right combination for your IoT environment

IoT deployments are complex but rewarding endeavors. There's a place for many permutations and combinations of sensors and styles of deployment. Industrial IoT applications often use many data inputs and many integrations customized to the specific situation and use case—from ensuring overall equipment effectiveness, to increasing manufacturing efficiency, to safety monitoring.

Deciding whether an enterprise will use fixed or dynamic sensing is another important consideration. This decision considers physical or safety limitations in the facility, the type of data being captured, the rate of change of relevant assets, budget, and many other factors—and these factors can change as data needs evolve. There is no one-size-fits-all option for IoT deployment. And with IoT projects projected to see meteoric growth, fixed and dynamic sensors will be effectively deployed in tandem to achieve the best results for an enterprise's goals.

Interested in dynamic sensing?

To learn more, please visit
www.bostondynamics.com

To contact sales, visit
www.bostondynamics.com/spot-sales

Footnotes

1. "State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally," IoT Analytics, May 18, 2022. https://iot-analytics.com/number-connected-iot-devices/
2. "How Much Does IoT Cost?" ITRex, September 6, 2022. https://itrexgroup.com/blog/how-much-iot-cost-factors-challenges/
3. "IoT Signals: Summary of Research Learnings," Microsoft, 2019. https://azure.microsoft.com/mediahandler/files/resourcefiles/iot-signals/IoT-Signals-Microsoft-072019.pdf