Microsoft

Capture value from the Internet of Things

How to approach a remote monitoring project

The Internet of Things (IoT)

The Internet of Things does not need to be complicated. It doesn't have to be about billions or trillions of devices. The Internet of Things is here today, and it's a practical and applicable technology trend that can generate return on investment (ROI) and drive efficiencies and insights for organizations that know how to use it.

Across the globe every day, businesses are connecting their assets and harnessing their data to create powerful new business value. Connecting devices is only the first step. The real value lies in the data that is transmitted from those devices, and the compelling business insights this data can enable.

These connected assets are producing large amounts of information. By tapping into the data streams and connecting them to the cloud and back-end systems, organizations can optimize business processes, make more informed decisions, identify new revenue opportunities, and understand and predict customer and partner behaviors in ways they couldn't imagine before.

At Microsoft, we believe the Internet of Things can make a difference to your business right now—beginning with the things in your business that matter the most. It's really the Internet of Your Things, and it starts by building on the infrastructure you already have in place, using existing devices and services in new ways, and incorporating the right technology to ultimately help you use data to create insights and make more informed business decisions.

The promise of remote monitoring

Imagine if your assets had eyes and ears, and could talk to you in real time. That's what IoT-driven remote monitoring offers. It involves collecting data from assets, and using that data to trigger automatic alerts and actions, such as remote diagnostics, maintenance requests, and other operational processes.

Why IoT is a game-changer

What used to be a manual, time-intensive procedure can now be dynamic, rapid, and automated. Now, assets located nearly anywhere can be monitored from afar. With live data from smart sensors and devices, organizations get better visibility into operational status, and can quickly, automatically respond to current conditions.

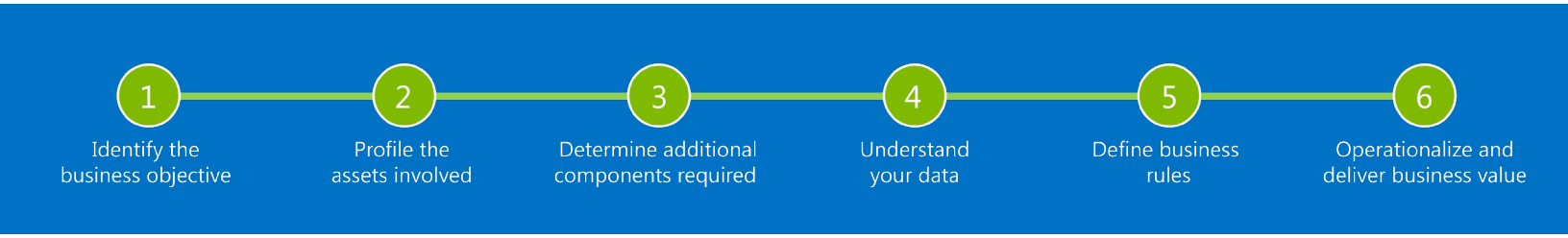
Benefits of using Microsoft Azure IoT solution accelerators for remote monitoring

With Azure IoT Remote Monitoring, you can connect and monitor your devices and analyze their data in real time to create new intelligence that can improve efficiencies and enable you to transform your business with new business models and revenue streams.

Get started quickly with Azure IoT Remote Monitoring to connect and monitor your devices in order to analyze untapped data and automate business processes.

A framework for getting started with remote monitoring projects

Each remote monitoring project will be unique—tailored to the needs of your business and your equipment. But at its core, the principles and considerations for a remote monitoring solution are very similar. In the next sections of this document, you will see details you should consider when getting started on a remote monitoring project.



1 Identify the business objective

Determine target business processes to improve, desired outcomes that monitoring should support, and other business case elements. Map out the end-to-end scenario and define high-level requirements.

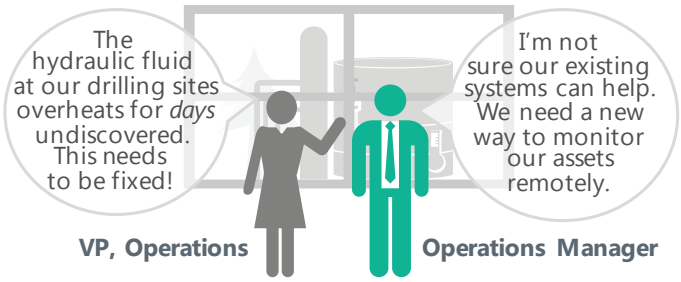
Line up executive sponsorship and get stakeholder support before moving into solution development to reduce the risk of a stalled project.

Start by determining the business objectives of your remote monitoring project. Examples include faster response times to equipment issues, or better insight into asset performance. The more specific you can be about the outcomes you want to achieve, the better. This is also a key part of the business case for the project.

When you've identified a business process you want to improve, identify elements of the process that an IoT remote monitoring solution could address. This likely requires analysis of the end-to-end business process—how it works today, where the inefficiencies are, and what changes you want to make.

For example, you might want a service alert or ticket to be created automatically if a temperature reading on a remote asset reaches a certain threshold. You'll need to identify the systems, tools, and teams that would need to be involved in making that possible, the requirements that need to be met, and the gaps and obstacles that exist.

This kind of analysis will help you determine the capabilities your solution must have, and will also indicate how extensive the business process changes might be. For example, if you want roaming maintenance technicians to receive real-time alerts of equipment problems, they need to be equipped with devices that deliver those alerts. And if you want technicians to respond immediately to alerts, their workflow will need to be adjusted to reflect that their priorities could dynamically shift if an alert comes in.



2 Profile the assets involved

Map and categorize your assets—consider asset types, where they are located, whether they connect in a secure fashion, and what data they are able to collect. Establish who has access to the assets and what kind of data they can view.

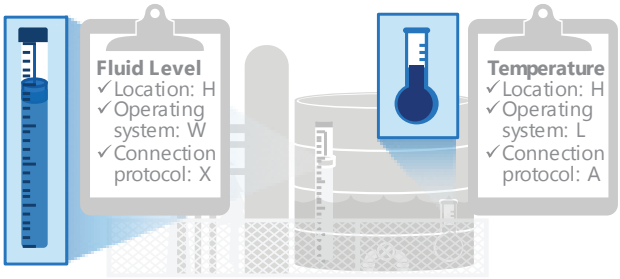
Ensure your solution can work with a variety of asset types and connection methods—both for assets you have and for assets you might add in the future.

Once you've identified the business process you want to address, you'll need to profile the assets involved. These might be smart devices at branch locations around the world, sensors on remote equipment, or even products installed at customer sites. There are a number of items that should be determined:

- **Types of assets**—high-value equipment such as manufacturing robots, automation equipment, or standalone sensors and actuators.
- **Operating systems**—such as Windows, Linux, Android, iOS, proprietary systems, or, in the case of "dumb" devices, no operating system at all.
- **Locations**—where the assets are geographically located and the environmental conditions they operate in.
- **Data**—what kind of data the assets can collect and send.
- **Connection protocols**—how the assets connect to internal systems or to a data storage location in the cloud.

Consider establishing a device registry, which enables you to define individual device identities and associate a specific device (or device group) with the data it generates. Mapping device characteristics lays the groundwork for establishing a device registry, and for device management and predictive maintenance capabilities.

It is also important to plan for device-level security, including who has access to what devices, and what data they can view.



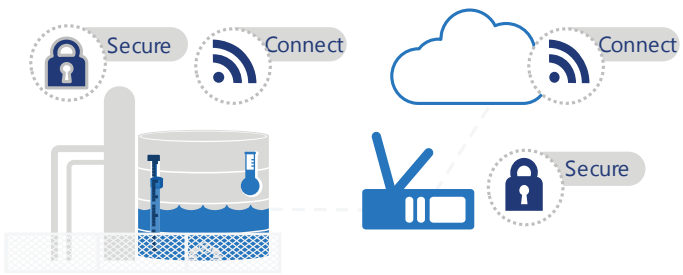
3 Determine additional components required

Set up additional devices if needed to connect sensitive or legacy assets. Plan end-to-end security. Assess the integration and development work required to address your business needs.

Additional solution components may include things like new sensors, or gateways, which connect to assets that use legacy communication methods.

Review critical elements of an IoT remote monitoring solution to identify any additional components your solution might require.

- **Establish connectivity to existing assets** that are not already connected to internal systems or to the cloud. In some cases, gateway devices may be needed to establish these connections. Gateways connect to assets that can't or shouldn't connect directly to business systems or the cloud. Examples include devices that use older or proprietary communication protocols, and assets that should not be directly connected due to security concerns. Gateways aggregate the data from these devices and send it to the appropriate location.
- **Plan end-to-end security**. Security measures should be in place to protect 1) data on the asset itself, 2) data in transit, and 3) the internal systems or cloud services where data is sent. Existing network security and identify/authentication measures may need to be extended to these assets if they are not already in place.
- **Assess the integration** required to address specific business needs. Integration with specific back-end systems and business applications is an important part of realizing value from remote monitoring, and from other IoT solutions, such as predictive maintenance.



4 Understand your data

Develop data profiles—including types and amounts of data your assets generate, how often new data is available, and where the data lives. Determine who needs what data, and how soon they need it in order for it to be valuable.

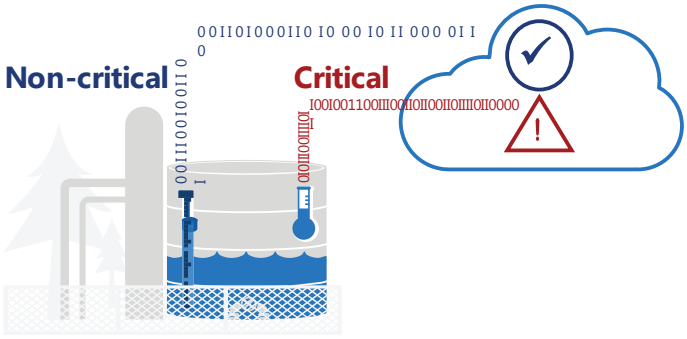
Determine which data needs to be sent to the cloud, and which data can remain on-premises. This will depend on a variety of factors, such as data volume and how quickly the data needs to be processed.

Understanding the data you can collect is an important part of validating that you can achieve the results you're looking for. Develop data profiles, which include:

- **Type**—data content (for example, temperature, level, vibration), format, and other descriptive characteristics.
- **Size**—how large the data files are that the asset will be transmitting.
- **Communication frequency**—how often data will be transmitted.
- **Location**—where the data will be processed and stored and, if applicable, how it will be shared across systems.

As you assess the data, you may find that you need to add or modify assets in order to obtain the data necessary to achieve your business goal. For instance, you may need to retrofit an asset with a sensor, or upgrade an operating system to enable data transmission.

Another important aspect of data assessment is to determine who needs what data, and when they need it in order for it to be valuable. In other words, which teams in your organization need which types of data, and how fast do they need it in order to derive the most use from it? Temperature data may be critical for an operations team to act on within hours in order to prevent spoilage. Data about the condition of an asset part with a long life may only be needed on a weekly or monthly basis. This information will influence how often data should be collected and transmitted for processing, and which systems must be integrated to ensure data is available to the right people at the right time.



5 Define business rules

Identify conditions that will trigger an alert, such as when data exceeds a threshold. Define the actions that should occur next—for instance, a technician is dispatched and given instructions on how to investigate the issue.

Consider business processes you wanted to implement in the past but weren't able to, like automated maintenance or responding to real-time alerts. These may now be possible.

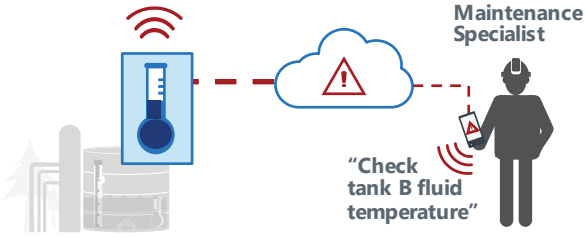
A key value driver of an IoT remote monitoring solution is the ability to define business rules—that is, the conditions or events that should automatically trigger an alert and/or action.

This requires identification of the specific data values that drive the trigger. For example, if temperature spikes above a certain threshold, or if temperature remains in a certain range for more than an hour. If you aren't sure precisely the right values to use, you can identify starting-point values, and fine-tune them as you learn more over time.

You also need to define the alerts and actions that should occur if a specified condition occurs—for example, if temperature exceeds a certain threshold, the nearest maintenance person is dispatched and given instructions on how to investigate the issue. If an asset can support two-way communication, the asset can take action—for example, if a threshold is exceeded, a command could be sent to the asset to run a diagnostic test.

In some scenarios, you may simply want an email or text alert sent to an individual or group. In others, you may want to ensure a person and/or machine takes action.

As you define business rules, make sure that the appropriate business process adjustments are also accounted for. As an example, if someone is responsible for acting when they receive an alert, how should they reprioritize their workload, and what is the expected response time?



6 Operationalize and deliver business value

Complete solution development and implement business process changes. Scale and integrate with back-end systems and applications. Gain real-time visibility and new insights, and use this information to improve operations.

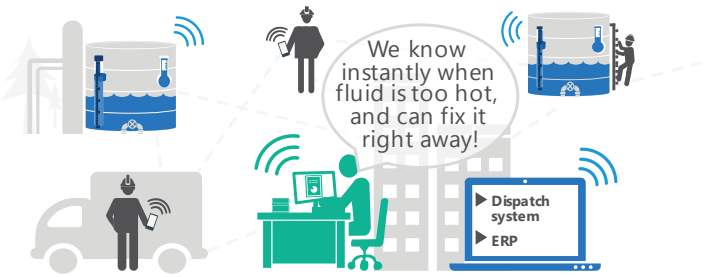
With sufficient data, you can identify problems and forecast events—the baseline elements for anomaly detection and, eventually, predictive maintenance.

After critical remote-monitoring solution elements are defined, the next phase is solution development and implementation. Starting with a pilot will enable you to validate the planned technology and business process changes before you scale. It will also enable you to refine your business rules and identify potential data gaps.

As you scale, you'll likely need to pursue additional integration with back-end systems and business applications. This will help you get the most value out of your solution. For example, if a product goes down at a customer site, an automatic service request could be logged in your CRM system. A service technician could then be notified to fix the issue or, if the data suggests that the machine needs to be shipped back for repair, then depending on the downtime costs for the customer you might also consider shipping a backup replacement product for your customer.

The benefits of remote monitoring vary, but often include near-real-time visibility into operating conditions, faster resolution of problems, and the ability to detect trends that weren't possible to see previously. All this contributes to cost savings and greater operational efficiencies.

Remote monitoring is also the starting point for predictive maintenance. The data gathered through a remote monitoring solution, particularly data that indicates normal conditions versus problem conditions, will enable you to build a predictive analytical model. This predictive model will be the foundation for a predictive maintenance program.



www.microsoft.com/IoT

Microsoft