Kaleido Intelligence

Honeywell

Light Report

Guide to IoT Connectivity for Industrial OEMs: Benefits & Needs

Introduction

IoT is affecting many different areas of business at a rapid rate, with over 2 billion connected devices in place at the end of 2021. This is bringing sweeping changes to many areas of work and personal life, and is a strong driver of industry 4.0 modernisation. Part of this includes connectivity becoming an increasingly important tool in asset management. Connected machinery can bring a range of benefits, from simplifying maintenance to driving energy efficiencies, ultimately producing a more reliable machine product experience. With these technologies increasingly available, industrial OEMs (original equipment manufacturers) need to understand how to leverage the technologies' capabilities to improve customer satisfaction and differentiate their products in the market.

Key to this is a range of capabilities that can be managed remotely by the OEM, taking burdens from the end-user. OEMs that can integrate the benefits of connectivity in their services can offer a differentiated and higher-quality product compared to traditional deployments with more manual and localised methods of operation. This can also contribute to new revenue streams for the OEM, thanks to the ready availability of data that can inform service delivery.

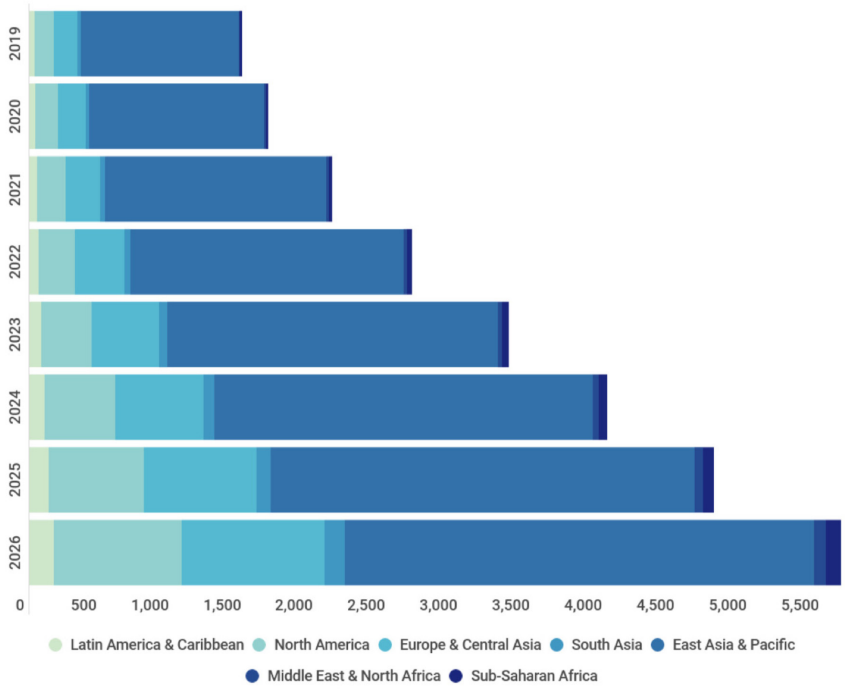
The key benefit of IoT in this regard is a range of ways to keep in contact with the end-user of the equipment. With the right IIoT (Industrial IoT) platform integrated into their assets, OEMs can become data vendors and partners with equipment end-users rather than being simple suppliers. This will drive engagement with their customers, making their company more visible and personable, as well as providing more efficient services.

Data Availability: A Two-Way Street

Both OEMs and customers can increase the visibility of their equipment through connected IIoT platforms, which can then form the basis for other services. This can give an OEM a better picture of the full extent of their deployments, and bring equipment management and optimisation into focus for end-users. It can also be beneficial for the OEM from a development standpoint: the feedback provided by the connected assets can then be leveraged in research and development efforts to enhance product designs.

This kind of solution requires clear data visualisation tools for the platform, as well as available APIs and data portals for the outputs to enable end-users to engage with the data in the way that is best for each enterprise's needs. KPIs can then be provided directly to both the OEM and the end-user, giving direct monitoring of equipment performance. Through this engagement, OEMs can collaborate with end-users to optimise deployments, benefiting the end user through increased efficiency, and the OEM by increasing their presence in customers' workflows.

However, getting at useful data is the first and most important step here. As experts on their own equipment, OEMs know what indicators provide the most actionable data to keep their products operating at peak efficiency. This means that any project aimed at data gathering for an OEM must be a dialogue, with connectivity providers relying on the OEM's guidance as to what data is necessary, rather than simply connecting equipment for connectivity's sake. These considerations will influence the entire IoT deployment, impacting not only what data is collected, but also how and when it is done.



Cellular IoT Connections in Millions, 2019-2026

Source: Kaleido Intelligence

Improved Maintenance & Efficiency

The ability to set safe operating parameters is one of the most immediately beneficial use cases for connected equipment, enabling automated alerts and other rules-based behaviours for the equipment that can bring maintenance from a reactive practise to a preventative one. This minimises unplanned downtime, making users' operations more efficient. The ability to provide a quantifiable ROI to IoT deployments through maintenance savings can be a key point in persuading end-users to buy into IoT systems. In addition, more responsive maintenance means that equipment lifecycles can be extended as damage caused by worn parts is easy to avoid. This saves money on capital expenditure as equipment will not need to be replaced as often as previously.

Given in to the hands of the end user, a live picture of equipment conditions allows for real-time adjustment of machinery, allowing quick and easy adjustments to equipment parameters, schedules and other elements of work. This gives the end user the tools they need to optimise the efficiency of their operations in line with their goals, whether that be to minimise maintenance times, increase production in anticipation of new stock coming in, adjust uptime in a schedule to minimise operational noise at particular times, take advantage of different electricity rates and more.

Remote monitoring is a key part of enabling this, meaning that reliable connectivity needs to be part of any successful IoT platform for OEMs. The data can then be relayed to the OEM's data hub, allowing them to react to any required servicing, replacement or other requirements shown by the data before problems arise. Any maintenance requirement can be understood before an engineer is dispatched, lowering the time spent diagnosing a problem. More extensive solutions will be able to also liaise with the end user, allowing for better co-ordination of schedules and increasing user engagement. Exactly how this can be done will vary from deployment to deployment, but if an OEM can provide that information in a flexible format as part of an end user's asset management, more points for engagement will be available.

New Business Models

Fully connected equipment can enable a range of new business models for both OEMs and their connectivity providers. With the improved maintenance and monitoring offered by cloud-based systems, service level guarantees can be far easier to provide. With this capability, OEMs can offer outcome-based service contracts to their clients, supported by the data and connectivity to carry them out.

The connectivity and analytics can also potentially be a revenue stream for the OEM. With the flexibility to view equipment conditions and the data they generate, data-related services can be provided by the OEM for their client to use, particularly if backed by systems that enable and enhance automation. As well as this, OEMs can use selected operational data as a platform to upsell customers, seeing when assets are operating at or close to their maximum capacity, and so can advise clients when more or different equipment is necessary.

Ultimately, this can feed into service-driven contracts, allowing equipment to be provided not as a capital expense, but as a monitorable service that is bundled with maintenance and upgrades as the client or equipment requires. The ability to monitor performance also means that levels of output can be reliably guaranteed in contracts, which will make any equipment usage more appealing from a business perspective. Even if this is not included at the contractual level, OEM visibility of these data means that replacement parts can be recommended for sale before the equipment fails, turning maintenance into an opportunity to upsell the end user.

Being able to offer flexibility in deployments is particularly useful in new business areas for an OEM or a client. In these situations, clients may not wish to fully commit to equipment purchases. The connectivity allows everything to be provided as a service, giving end-users the option of trial and flexible deployments rather than expensive CAPEX commitments to new project work.

Planning Needs

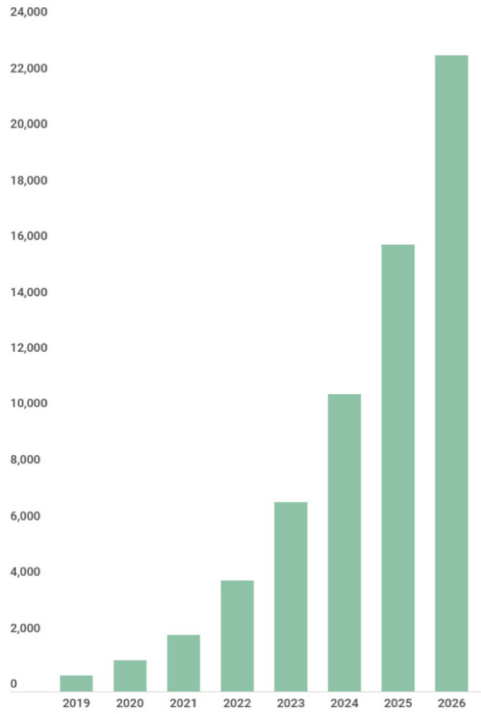
Despite these benefits, increased connectivity brings additional complexity to equipment production and management. There are three elements to assess to ensure that the deployment will achieve its full potential for an OEM:

1) **Strategy** – What is the end goal of connecting the assets? This requires an evaluation of what data can be collected, and how that data will be used. This is particularly important for the commercial element of any IIoT deployment, most particularly if any data needs to go to the cloud. Securing any edge processing and connections to cloud infrastructure ensures that the data being gathered and any attendant connectivity serves a distinct commercial purpose, as well as safeguarding any sensitive data.

2) **Assessment** – What are the assets that are to be connected capable of sending the required data? This is a necessary step to ensure that the required data are something that the equipment can actually gather. In addition, data transfer policies need to be evaluated to see how data can be collected and whether that is done securely.

3) **Redesign & Changes** – Following on from the assessment, the question of whether and how to redesign equipment to enable data collection and transmission needs to be addressed, covering what additional components, sensors, and forms of connectivity need to be added to devices in order to perform their function. This step needs to incorporate elements from the previous two stages to keep any redesigns fully focused on the outcomes.

This kind of connectivity could be particularly well-suited to a private network deployment, providing additional security as well as inclusive connectivity. Private cellular networks are an increasingly attractive option for many industrial use cases, and they can enhance any quality-of-service based platforms, through the ability to extend and guarantee a level of service across an end user's entire facilities, mitigating several of the problems that Wi-Fi and public cellular networks bring.



Number of Non-Public Networks Deployed, 2019-2026

Source: Kaleido Intelligence

The assessment necessary to properly understand and deploy connected equipment is not a simple undertaking, and users' expectations need to be managed. The connectivity and data gathering both need to be fully validated before data can be used operationally, which can take time to implement. Part of any planning needs to also incorporate a timescale for the improvement that the IIoT will bring, which will often be several months before gains can be realised. This will often be more if equipment redesigns and modifications are required.

Infrastructure Needs

The monitoring requirements of connected equipment typically will involve interactions with a cloud server for the OEM to access data to co-ordinate its operations. This requires a secure cloud through which to pass the data before usage by the OEM and their clients. This will frequently mean outsourcing such computing expertise to another company, and can easily be implemented into a full end-to-end management platform to keep operations simple.

The security element is vital, as simply connecting equipment without bearing security in mind will inevitably leave vulnerabilities that can be exploited. It is also one of the bigger concerns for those end-users connecting their infrastructure for the first time, and so being able to provide a strong security posture as part of a deployment is necessary in many ways. This means both equipment and connectivity security, as well as an ability to have visibility into the full network.

Finding services that can integrate legacy ICS (industrial control systems) into the connected ecosystem is a key component in this process, and will be for many years until connected assets become the default, and older devices are frequently a vector for cyberattacks. The most obvious way to combat this is through bringing in new interfaces with embedded cyber security compliant with IEC62443-2 standards along with secure connectivity with protocols such as MQTT Sparkplug B, but this is often not possible. This makes it imperative that any connected asset strategy has the means to incorporate legacy equipment, either by adaptation of hardware or through an interface that can accept a wide variety of inputs from many different vendors. This lessens the need to entirely replace an equipment range in order to leverage connected services. This makes asset discovery and onboarding a key competence for any digital OEM solution.

It also requires that the data be easily viewable both as a whole for OEMs to have full visibility of their assets, and on a per-client basis to provide data, services and billing to their customers. It also means that any connectivity platform needs to be based on common standards, or at least able to incorporate protocols other than its own into the managed equipment ecosystem. Without this ability, management platforms risk leaving some assets unable to interact fully with the OEM's systems.

Operational Needs

OEMs frequently do not have the in-house expertise to complete this process themselves, and so it becomes vitally important to find a technology partner that can provide end-to-end digital execution and ongoing support, to ensure that the OEM's operations can remain simplified throughout the device life cycle. This is particularly important for small and medium-sized enterprises, which will not have the ability to immediately manage the platform and may never have the capability to develop end-to-end network design and management skills. Without a reliable partner, these players will hve to find the resource to upskill their existing workforce to handle the data, with changes necessary both for the OEM and their customers.

The ability to have an ongoing relationship with a partner throughout the digitisation process is also key, to ensure that the right elements are being measured in the right way. Such a relationship can also include the training necessary for end users and OEMs to fully leverage their connected equipment. The best partners in this space will remove the complexity that connectivity brings while engaging in a dialogue with clients to ensure that their OEM clients are getting the best from their connected assets.

Conclusion:
Simplicity & Compatibility are Keystones for Extending the IIoT

Connected equipment has many benefits to offer organisations of all sizes, and can transform how the OEM market operates if implemented correctly. However, in order to realise those gains technology partners need to be able to work with OEMs where they are now, and at all stages of IoT deployment and execution. This has been accelerated by COVID-19, but the change is far from over. OEMs and technology providers need to work collaboratively on deployments, incorporating current technology and understandings, in order to derive the maximum benefit from these new technologies.

> Honeywell Connected OEM