THE INDUSTRIAL IOT IS DRIVING ECONOMIC GROWTH

By Philip Ling | January 14, 2022

Manufacturing businesses stand to make tremendous gains by adopting Industrial Internet of Things (IIoT) technologies. Ignoring the transformative opportunity risks competitive disadvantage, given that other companies in the same space will grab the opportunity to become more efficient and productive.

According to a report by Accenture, the Gross Domestic Product of the U.S. could increase by more than $7 trillion by 2030 due to the efficiency and productivity gains on offer, while globally gains could go up by over $14 trillion.

Automation data is now much more accessible thanks to the Industrial IoT, and it is driving economic growth as well as digital transformation.

How did we get here?

A thirst for knowledge relating to industrial processes existed since the first factories went into service. Manufacturing has always been about increasing productivity and, while initially a low priority, improving safety.

However, good data to support those goals can still be difficult to liberate from factory assets traditionally isolated within closed industrial control systems or supervisory control and data acquisition (SCADA) systems.

The IIoT changes that. It introduces a flexible concept that encompasses technologies including sensing, networking and communications, and combines them with computing and analytics. This enables solid connections between the factory's operational technology (OT) systems and to the enterprise information technology (IT) domain. It's the critical enabler for companies to achieve digital transformation and is the essence of the fourth industrial revolution.

Bringing key ingredients together is what really differentiates the IIoT from traditional ways of capturing and analyzing manufacturing data. The technologies include:

- Smart, digital sensors that are affordable to deploy in the huge numbers needed to monitor almost any parameter in an industrial environment or process: motor speed, vibration, inspection data, etc.
- Wireless networking technologies include point-to-point and mesh networking that allows connecting large numbers of sensors with minimal additional cabled connections, which can be disruptive to install and potentially unreliable.
- IIoT-friendly communication protocols such as Open Platform Communication Unified Architecture (OPC UA), which is platform-independent and leverages internet standards such as TCP/IP and HTTP(S) that promote seamless machine-to-machine communication.
- Low-power IC technologies, as well as energy harvesting and storage, that enable deployment in almost any location.
- The accessibility of high-performance computing, affordable even to small organizations on an "as-a-service" basis, in the cloud and moving toward the edge (including AI, which is well suited to pattern recognition tasks that are fundamental to analyzing sensor data).
- Developments in data science, aided and abetted by the ongoing increases in computing performance to capture and crunch vast quantities of data (Big Data) from ubiquitous sensors. This can reveal otherwise undiscoverable insights into the numerous causes and effects that occur within every process happening inside the factory.

What can the IIoT do now?

An effective IIoT program lets manufacturing businesses monitor equipment and process performance continuously and in minute detail. Data – both real-time and historical – can be acquired and analyzed. Other sources from across the business, the wider supply chain and the outside world can augment the sensed data. Analytical applications then bring these disparate data sets together and detect patterns among the huge numbers of variables that would be practically impossible to analyze using traditional methods.

This data can be used to improve the performance of processes in action on the factory floor. It works by capturing vast numbers of machine parameters, settings, adjustments and environmental data like temperature and humidity. This can be combined with other types of data, such as the operator's ID. The results of the analysis can be used to identify opportunities, to fix problems and improve manufacturing performance.

THE INDUSTRIAL IOT IS DRIVING ECONOMIC GROWTH

By Philip Ling | January 14, 2022

Intelligent condition monitoring captures data about the operation of individual items of equipment, such as machine tools, to identify when adjustments or repairs may be needed. Pre-IIoT technologies could cope with this on a basic level such as detecting excessive vibration in a motor shaft that could indicate impending failure. The action is to trigger a predictive maintenance call that allows the item to be replaced at a convenient time thereby avoiding unplanned downtime and the associated expenses such as lost production and emergency repairs. IIoT technologies make this much easier to arrange and more reliable, given the ability to monitor larger data sets and extra variables.

Moreover, with pervasive sensing and real-time continuous data capture, equipment vendors can intensively monitor a specific asset installed at a customer site and generate a virtual digital twin to analyze and anticipate its needs and identify trends. This ultimately builds a closer relationship with the customer to improve service and deliver greater value. Customers can experience consistent optimal performance, increased reliability, improved productivity, delivering a greater and faster return on their investment in equipment and services.

The insights into manufacturability, which can be gained by analyzing historical data, also assist new product design. Information about process issues and remedies can guide the design of subsequent products to prioritize successful processes and avoid any that have proved to be problematic. Working with a digital model lets the service provider try various new ideas, perform experiments, or change the operating conditions virtually to evaluate upgrades and identify new applications.

What are you waiting for?

Leveraging IIoT technologies to create a smart factory offers tremendous opportunities. On the other hand, IIoT's almost limitless scope and complex many-faceted nature can present barriers to taking that first step. There is the prospect of installing and onboarding thousands upon thousands of sensors, noting also that legacy equipment can present barriers to implementation. Then there is the challenge of managing the data produced. Each machine in a factory could generate as much as 5GB of data per week, amounting to about 5 petabytes (5 million GB) across all assets in a typical factory.

Starting small may help. Begin by collecting data from selected equipment or processes (perhaps the easiest to understand or those known to be under performing) and connect to cloud-based analytics services. Working with a partner that can offer various building blocks and services can demystify and shorten the learning curve. Avnet has a variety of proof-of-concept platforms with flexible connectivity options ready to start sending data to the cloud. Real-time analytics applications, REST APIs and SDKs are also provided for easy development, and lifecycle services are available to accelerate implementation and aid maintenance.

Moving forward, test programs can scale quickly by adding more sensors, monitoring additional equipment and processes, and performing more diverse analyses. Also, the value of the data can be assessed or filtered to capture events of interest. Basic data processing and filtering can be done at the edge of the network using edge controllers, smart gateways or aggregators. This can reduce network traffic, data storage and cloud workload, as well as enhance real-time performance.

The diverse elements of the project require specialist expertise, which may not already reside within the organization. Engaging external consultants or recruiting new skills may be necessary to assemble competencies covering sensing, networking, computing and security.

Potential cyberattack is a given for online assets, putting safety and financials at risk. Initiatives such as the U.S. NIST (National Institute for Science and Technology) Cybersecurity for IoT Program and associated NISTIR 8259 recommendations are helping the industry respond effectively to cyberthreats. One example is that IoT-focused embedded processors and SoCs now routinely incorporate hardware-anchored features to support secure booting and firmware update. However, installers must also remember to change the manufacturer-default passwords of newly installed devices. Often neglected, this can effectively block casual hackers and greatly reduce the attack surface.

Conclusion

A 2019 report on the IIoT commissioned by the U.S. Department of Homeland Security estimated the number of connected IoT devices at over 27 billion. It's a huge opportunity although daunting in scale and diversity, with significant risks such as security that must be addressed properly. On the other hand, manufacturing businesses must learn to harness its benefits to continue increasing productivity and compete in the marketplace. The challenge is too complex for most companies to tackle organically. A trusted partner capable of providing solutions, expertise and long-term support is a critical ingredient for success.

Avnet
2211 S. 47th Street
Phoenix, AZ 85034
1-800-332-8638
avnet.com