

The Beginners Guide to IIoT

A 101 guide outlining the features, functions and benefits of an Industrial Internet of Things (IIoT) Platform.

[WATCH A DEMO](#)


What is the IIoT (Industrial Internet of Things)?

The Industrial Internet of Things (IIoT) refers to all the industrial devices used in manufacturing that are connected to wireless networks, gathering and sharing data. This includes machines in factories, engines in airplanes, and robotics. IIoT enables industries to use the data gathered and shared by these devices to be more efficient and reliable in their operations. To employ IIoT in your business and improve your processes, you need to understand the role it plays in manufacturing. This guide covers what IIoT is, why it's important, and what to consider when investing in an IIoT platform. In this article, we will also reference a user study that involved 49 one-hour in-depth phone interviews with senior management, operations execs, and manufacturing engineers. This study was carried out to identify the current state of IIoT in manufacturing, challenges, solutions, and recommendations.

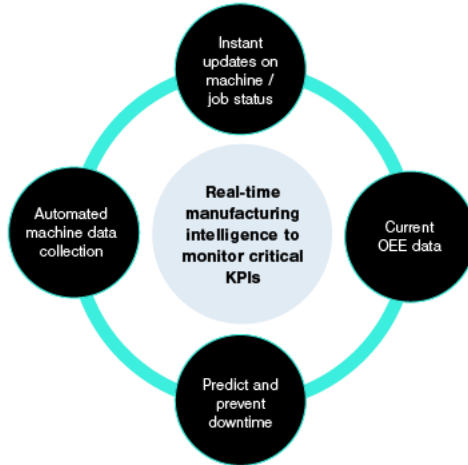
What Does IIoT Mean?

The Industrial Internet of Things describes the use of the Internet of Things (IoT) in industrial sectors and applications. IoT refers to the billions of devices around the world that are connected to the internet, collecting and sharing data. IIoT goes beyond the physical devices usually associated with IoT. What makes it distinct is the convergence of information technology (IT) and operational technology (OT). OT includes industrial control systems (ICSs), for example, human machine interfaces (HMIs), supervisory control and data acquisition (SCADA) systems, and distributed control systems (DCSs). IIoT platforms use big data and analytics to transform production processes. Having a dashboard that provides a strategic overview of the devices, machinery, and robotics used on the factory floor helps reduce downtime, improve efficiency, and inform decision making.

The Industrial Internet of Things helps businesses achieve a Smart Factory. Smart Factory is a concept used to express the end goal of digitalization in manufacturing. According to our user study, Smart Factory was the preferred umbrella term for the IIoT platform PLEX provides. A manufacturing process that uses the highly digitalized IT and OT to collect and share data is referred to as a Smart Factory. An example of IT that helps businesses achieve Smart Factory is machine automation. Machine automation is designed to control the work of machines, with in-built computers that improve the quality of products and services, increase productivity, and allow workers on a shop floor to concentrate on less menial tasks.

 Welcome back ! Are you ready to get started with Plex?

Why is IIoT Important?



The IIoT is important because it helps manufacturers overcome common challenges with production and plant throughput. In our study, we asked respondents what their biggest challenges were; the most common responses included labor shortage, COVID-19, asset downtime, training new staff, and poor forecasting. Using IIoT platforms to provide extremely detailed data in real-time can help companies better understand their current manufacturing processes and make improvements in line with the information provided. A more productive and efficient factory floor will open new revenue streams. The IIoT can also gain insight into the broader supply chain, allowing businesses to implement further efficiencies. IIoT platforms improve uptime, efficiency, and yield, while reducing labor dependencies.

In our user study, we provided respondents with a PLEX IIoT solution. Our solution features a dashboard where users can monitor machine health in real-time, including machine uptime, state, part, and job. The dashboard also includes contextualized machine data, providing current and historic values such as job number, part number, and workcenter status. PLEX's comprehensive solution provides alerts and historical analysis, meaning users can gain visibility into live historical sensor data for machine health and get maintenance alerts across a wide set of equipment. Use this information to track OEE and reduce costly downtime.

After we showed our IIoT solution to respondents, survey results highlighted a real need for this technology. We asked them to rate their interest and how important they felt our solution was for their business from 1-7 (*1 low – 7 high*). On average, those from large companies rated our solution as 6 for interest and 6 for importance. People from smaller businesses rated it as 6 for interest, 5 for importance.

This shows a real need for this technology amongst engineers and execs once they have been shown the value IIoT can bring to their business. One of the key challenges to this type of platform is that not enough manufacturers are aware of IIoT platforms and their importance. When broken down by sector, 92% of manufacturing engineers identified a need for PLEX solutions, 81% of operations execs said the same, and 83% from IT also expressed a need for this technology.

7



Collaboration & Processes
Involving people & business processes

6

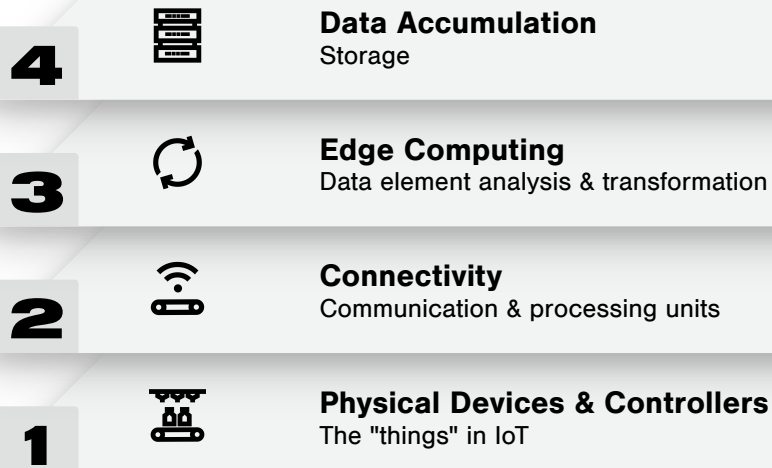


Application
Reporting, Analytics, Control

5



Data Abstraction
Aggregation & Access



IIoT Considerations and Challenges

While the IIoT platforms can revolutionize operations, maintaining security for a digitalized Smart Factory can be a challenge. Integrating operational technology to the internet sees the introduction of more intelligent and automated machinery. This in turn invites a range of new challenges that require a deeper understanding of the IIoT. Three areas need to be focused on when adopting a new solution: availability, scalability, and security. Many businesses may already be familiar with availability and scalability when it comes to industrial operations, but security is a potential hurdle when it comes to integrating the IIoT. For example, many businesses still use legacy systems and processes which have been in operation for decades, which complicates the adoption of new technologies.

Another potential challenge is that acquiring new smart devices gives rise to security vulnerabilities and accountability. Businesses adopting the IIoT are responsible for the security of setting up and connecting the new devices and should be able to ensure the security of the users and provide the necessary response when issues arise. Using an increased number of smart devices in business operations creates an increased risk of data breaches, for example, hackers gaining access to these connected systems. This type of major breach can lead to a shutdown of operations, and the necessary cybersecurity steps must be taken to protect against incidents such as this.

Finally, businesses should also be made aware of the risks that come with using data. The IIoT uses a huge amount of data to inform business decisions and help streamline certain processes, but it is essential that personal information is kept separate from general log data. User data should be processed in accordance with privacy regulations, such as the European Union General Data Protection Regulation (GDPR). All personally identifiable information (PII) should be kept in a protected, encrypted database. Businesses looking to adopt the IIoT as a solution should consider the following risks:

- **Software vulnerabilities that can be exploited by hackers**
- **Publicly searchable internet-connected devices**
- **Threat from hackers, targeted attacks, and data breaches**
- **System manipulation that can cause operational disruption and sabotage processes**
- **System malfunctions that can cause faults in devices, damage to facilities, and injury to workers**

The more connected devices adopted by a company, the more security risks. Considering all the potential risks during integration is essential.

How Do You implement IIoT?

We have discussed the potential risks, but what can businesses do to successfully implement IIoT and mitigate the security risks? Having a security operations center (SOC) is vital for monitoring and defending against the risks we listed above. This allows industries to oversee, encounter, and respond to a high number of security alerts. A SOC team detects security issues or anomalous activity and

immediately addresses issues before they cause any damages. Businesses may want to take this a step further and hire a dedicated security team for tackling security issues specific to an operations technology environment. Hiring a specialist team who understand the threats of adopting the IIoT offers business the best possible protection from security risks. Having full stack protection built into different layers of IIoT implementations, such as device, the network, and the cloud, should be a security objective. This allows industries and manufacturers to securely conduct their operations.

The device layer incorporates the devices and applications that businesses use to implement the IIoT. These are supplied by manufacturers and service providers, and businesses should understand how their suppliers transmit and store data. This way, manufacturers and service providers can notify IIoT adopters of any security issues and how to handle the situation.

The network layer includes a gateway that gathers data from different connected devices. Businesses looking to implement an IIoT solution should have next-generation intrusion prevention systems (IPSs) monitoring and detecting potential cyberattacks. Control centers are kept in the gateway and used to issue commands to connected devices. This is where organizations should look to implement their security systems.

The cloud layer is where organizations should implement security that runs server-based protection to mitigate the risk of hackers accessing servers and sensitive data. Implementing IIoT systems correctly and overcoming security risks requires connected threat defense from the gateway to the endpoint, that can provide:

- **Regular monitoring and detection**
- **Threat visibility and anomaly detection**
- **Prevention of threats and attacks between IT and OT**
- **Secure data transfers**
- **Next generation intrusion prevention systems**
- **Server and application protection across the data center and the cloud**

Industries and manufacturers who are aware of the risk and are willing to invest in the integration and security of new IIoT systems are the ones most likely to see a successful implementation of this technology.

IIoT and MES

There is no doubt the IIoT is having a big influence on manufacturing, spurring initiatives, pilots, and studies around the world. This has led to concerns that IIoT could replace existing manufacturing execution systems. It's important that industries understand that the IIoT can complement MES, rather than replace it. In many cases, the IIoT can expand the capabilities of MES, using smart devices and cloud-based systems to reduce downtime, increase overall equipment effectiveness (OEE), and satisfy a greater need for return on assets. There are currently gaps in MES that can be positively filled by the IIoT, for example, manufacturers may find the data from their equipment stale or untrustworthy, and accessing the data is very expensive. The IIoT should be seen as technological progress, and introducing smart sensors, actuators, and more reliable cloud infrastructure will only improve the performance of MES. It's important businesses realize that they can use this technology to complement their current MES software, and not see it as a replacement. Here are some examples of how industries can look to integrate the IIoT with MES:

- **Move MES away from being a standalone application, integrating many technologies.**
- **Test IIoT technologies that could improve the MES.**
- **Test IIoT applications for measurable gains in productivity.**

The IIoT could be the future of MES, so industries need to be open minded when it comes to integrating new technologies within their business.

This article provides deeper insight into the IIoT and why it is important for businesses. Using PLEX's analytics and IIoT can help you reduce costs, increase profitability, drive revenue, and more. You can learn more about PLEX solutions and leverage the full benefits of analytics coupled with IIoT [here](#).

An IIoT Example

To better understand the IoT World Forum Reference Model and the way this technology can be applied to a manufacturing plant, we have put together an IIoT use case. Let's say you are a manufacturer of metal automotive parts. Here's how information might flow in your plant.

Layer 1: Physical devices and Controllers +

Layer 2: Connectivity +

Layer 3: Edge Computing +

Layer 4: Data Accumulation +

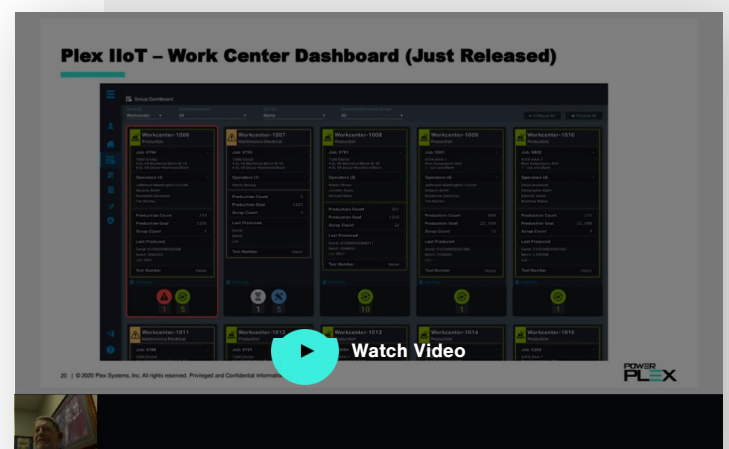
Layer 5: Data Abstraction +

Layer 6: Application +

Layer 7: Collaboration & Processes +

IIoT Case Study

Still looking for more examples of IIoT technology in manufacturing? Check out this on-demand session from PowerPlex in which Bob Bierwagen VP of Strategy for MPI Corporation, provides an overview of how the IIoT journey got underway at MPI, what they have learned over the past year, what the future holds, and how MPI is benefitting from the effort.



You'll walk away from the session with an understanding of:

- The drivers for adopting Industrial Internet of Things.
- How the pilot project was selected and defined.
- The development of a high-level business case as well as lessons learned along the way.

MPI Corporation Shares Their IIoT Journey

Frequently Asked Questions

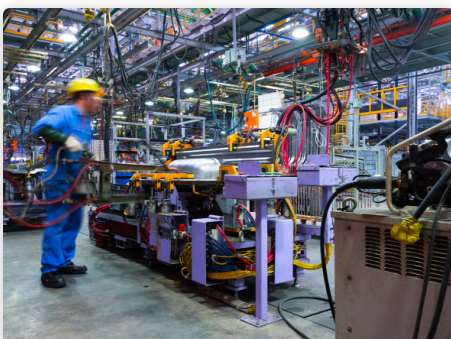
What is the difference between IIoT and IoT?

The main difference between IIoT and IoT is how they're used. IoT is mostly used by customers or end users, while IIoT applies to industrial purposes such as manufacturing, monitoring and supply chain management.

What are the benefits of IIoT adoption?

How does IIoT work?

Learn More About IIoT

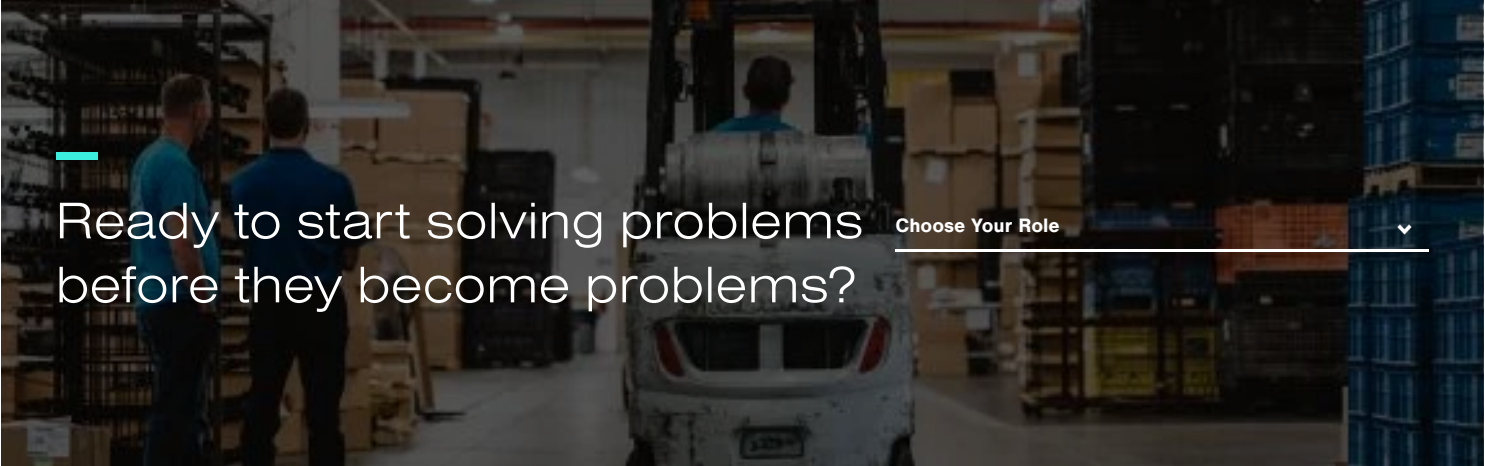


Ebooks

Three Ways Industrial IoT (IIoT) Yields Bottom-Line Benefits

Brochures

Plex Asset Performance Management (APM)



Ready to start solving problems before they become problems?

Choose Your Role



Products

Manufacturing Execution System (MES)

Enterprise Resource Planning (ERP)

Quality Management System (QMS)

Supply Chain Planning (SCP)

Production Monitoring

MES Automation & Orchestration

Asset Performance Management (APM)

Platform

Smart Manufacturing Platform Overview

Cloud Infrastructure & Security

Mobile Application

Availability & Performance

Manufacturing Automation

Industries

[Automotive](#)

[Food & Beverage](#)

[Precision Metalforming](#)

[Plastics & Rubber](#)

[Industrial Manufacturing](#)

[High Tech & Electronics](#)

[Aerospace](#)

Resources

[All Resources](#)

[Success Stories](#)

[Analyst Reports](#)

[Knowledge Articles](#)

[Demos](#)

[Blog](#)

Services & Support

[Customer Success & Advocacy](#)

[Support Services](#)

[Education Services](#)

[Professional Services](#)

[Plex Community](#)

Company

[About Us](#)

[Customers](#)

[Partner Ecosystem](#)

[Newsroom](#)

[Events](#)

[Careers](#)

[Contact Us](#)

Knowledge Articles

MES Beginners Guide

Cloud-Based MES Basics

What is a Quality Management System (QMS)?

Types of Quality Management Systems

IIoT Beginners Guide

What is Industry 4.0?

What is Connected Manufacturing?

What is a Smart Factory?

The Rise of Automation in Manufacturing

The Future of Robotics and Automation in Manufacturing

Supply Chain Planning: a Guide to Strategic Planning and Operations

What is Smart Supply Chain Management?

An Extensive Guide To Asset Performance Management (APM)

A Guide to Monitoring Machine Performance



888.454.7539