How to get started with IIoT

Cloud connectivity on the factory floor

By Will Dietz, Product Manager, IMA – Automation Infrastructure Market Development, Phoenix Contact Development and Manufacturing, Inc.

Learn more about

- The challenges of IIoT integration
- The benefits of IIoT
- Cloud connectivity
- Best practices for implementing IIoT connectivity

Introduction

Industry 4.0 and the technologies behind it represent a paradigm shift in manufacturing. Companies create value by leveraging technology, from cloud computing to artificial intelligence to the industrial internet of things. But adoption isn't always a straightforward process.

The factory floor relies on proven technology and incremental process improvements rather than adopting developing technologies and disruptive ways of working.

Manufacturers continue to rely on legacy machinery and equipment. Industrialists prioritize reliability for uptime and worker safety. Organizations recognize the driving forces: modernization and digitization are necessary to remain competitively viable, but these emerging IT-driven solutions are not a core competency for many companies.

That's why we're going to break it down for you.

This white paper covers everything you need to know to get started with cloud connectivity and IIoT on the factory floor.

Figure 1: A digital twin is a virtual representation of an object or system.

From going through the challenges and benefits of IIoT to understanding key technologies and best practices, you'll gain a foundation that will help you understand your options, plot a strategy, and move forward.

What is IIoT?

The Industrial Internet of Things (IIoT) is an Industry 4.0 technology that integrates industrial machinery and equipment with internet connectivity and advanced sensors.[1] This enables data collection, analysis, and advanced automation in industrial environments.

Networking is a hallmark of IIoT; connected devices talk to each other on the plant floor for real-time edge computing analysis and process optimization. At the same time, they can also send either streaming data or aggregated reports to the cloud for big data analysis, digital twin creation, and other strategic use cases. (Figure 1)

IIoT enables manufacturers to more thoroughly connect, monitor, and control their factories.

That's why IIoT is already revolutionizing heavy industry. Smarter, more connected factories empower both decision-makers and technicians with real-time data, automation capabilities, and actionable insights.

This leads to increased efficiency, improved productivity, reduced costs, and smarter decision-making. ■

continued →

Contents

The challenges of IIoT integration

Successfully implementing IIoT on the factory floor requires overcoming technical, workforce, and security challenges. This is how manufacturers scale IIoT beyond an initial pilot program.[2]

Technical challenges

First, we have connectivity and network infrastructure. Remember, the Industrial Internet of Things won't function without that crucial internet component. IIoT relies on robust and reliable network infrastructure, such as Industrial 5G, to connect and communicate with devices and sensors.

It's challenging to establish a stable and secure network that can handle the volume of data generated by numerous connected devices. According to PwC, the "global growth curve for the industrial IoT is set to rocket towards 100 billion devices as the technology becomes pervasive in industrial sectors worldwide."[3] With so many devices on a network, it's crucial for manufacturers to invest in high-bandwidth, low-latency solutions.

Figure 2: The IT and OT teams bring different perspectives to an IIoT application, but collaboration and communication can bridge the gap.

Additionally, ensuring adequate network coverage and resolving potential connectivity issues in large factory environments or remote locations may pose further challenges.

Second, interoperability and standardization are also a concern. Between the wide range of IIoT solutions hitting the market and the fact that many factory floors include a variety of legacy systems, equipment, and machinery from different manufacturers, getting everything to work in unison is a challenge. Add the fact that these legacy systems each have their own proprietary protocols and interfaces, and the complexity balloons even further.

System integrators must find creative solutions to introduce standardization and interoperability. Common communication protocols and data formats, for instance, can help address these challenges.

Third, there's the issue of legacy system integration. The average life span of operational technology (OT) is generally much longer than that of information technology (IT). And, mentioned previously, most factories rely on legacy systems that were not designed for connectivity or communication with other systems.

IIoT integration can be challenging. This often means retrofitting or adding gateways to enable connectivity and data exchange.

Addressing these technical challenges requires careful planning and close collaboration between OT and IT teams. It also demands a thorough understanding of the factory floor's specific requirements.

Harnessing the potential of IIoT for the factory floor requires selecting the right technologies, implementing robust security measures, investing in infrastructure upgrades, and leveraging advanced analytics and automation tools.

At the same time, it also requires a workforce with a diverse skill set. Companies need talent with expertise in areas such as networking, data analytics, cybersecurity, software development, and system integration.

Workforce challenges

First, IIoT is a relatively new field and a rapidly evolving technology. New devices, protocols, and standards regularly emerge. Keeping up with these advancements requires continuous learning and upskilling, which is a challenge for both organizations and individuals.[4]

Higher education programs are popping up to fill this gap, but, especially in their interim, organizations will need to invest in learning and development (L&D) in their existing workforces as they make the switch to Industry 4.0.[5]

Second, IIoT requires multidisciplinary knowledge that spans both IT and OT. Bridging the gap between these domains and fostering collaboration between traditionally separate IT and OT teams poses a significant challenge. (Figure 2)

While there are formal education programs that focus on IIoT skills, there are limited opportunities for students to become IIoT engineers in the same way they may focus on mechanical, electrical, or chemical engineering.[6]

continued →

Traditional academic curricula often lag behind the rapidly changing tech landscape, making it difficult for institutions to provide graduates with the skills necessary for IIoT implementation.

Finally, there's the challenge of industry-specific expertise. Every vertical has its own unique requirements and challenges when it comes to implementing IIoT. That industry-specific knowledge and experience are critical for a successful IIoT program. However, finding professionals who have both IIoT expertise and industry-specific experience is a difficult task.

The last main set of challenges comes down to security. Widespread IIoT adoption introduces various security challenges.[7] Organizations must ensure the confidentiality, integrity, and availability of data and systems.[8]

This is especially true considering the current geopolitical climate in which nation states have launched attacks against other countries, such as Russia's NotPetya malware that took down Ukraine's power grid and inflicted collateral damage across the globe.[9]

Security challenges

Of course, cybersecurity threats make the top of the list. IIoT devices and networks may be vulnerable to a wide range of threat actors, including malware, ransomware, distributed denial-of-service (DDoS) attacks, intrusion, and data exfiltration.

These threats can disrupt operations, compromise sensitive data, and even compromise access controls to critical systems. Case in point: in 2021, a cyberattack forced the shutdown of a top U.S. pipeline.[10]

Unauthorized access is another major challenge. IIoT devices often have multiple entry points, or attack vectors, open to potential attackers. These can include weak or default passwords, inadequate authorization and access controls, or unpatched vulnerabilities.

Threat actors may exploit these vulnerabilities to gain access to devices, from which they can move laterally through the network to establish persistence. Unauthorized access can lead to data manipulation, the ability to control equipment, or theft of sensitive information.

Data privacy concerns pose an additional challenge to security. IIoT generates and collects massive amounts of data, including sensitive and/or proprietary information from operations and production. Ensuring the privacy of this data is crucial, as unauthorized access or data breaches can result in financial loss, reputational damage, or regulatory noncompliance.

Compliance with data protection regulations, such as Europe's General Data Protection Regulation (GDPR) and the patchwork of statewide regulations that continue to emerge, is essential for organizations that handle personally identifiable information (PII) or other personal data that's collected through IIoT devices.[11,12] ■

Benefits of IIoT

The benefits of working through the challenges of implementing an IIoT strategy result in several key factors.

First, IIoT enables data-driven insights. These devices collect real-time data from sensors that are embedded into machines, equipment, and other assets on the factory floor. The access to real-time and actionable data provides a clearer picture of operations than we've ever had before.

The result is that companies can analyze the data to extract valuable insights into the performance, efficiency, and condition of their machinery and operations. Manufacturers can identify patterns, detect anomalies, and make informed decisions to optimize production processes, reduce downtime, and improve overall productivity.[13]

Speaking of reduced downtime, the second benefit is predictive maintenance. This means that manufacturers can monitor equipment and predict failures before they happen, giving them a window to complete preemptive maintenance or repairs.[14]

This proactive approach prevents unplanned downtime, reduces maintenance costs, and increases machinery life spans.

The third benefit is enhanced automation and efficiency. IIoT facilitates the automation and optimization of various processes on the factory floor. By connecting machines and devices, manufacturers can streamline operations, enable seamless communication between different components, and automate tasks that previously required manual intervention.

This leads to improved efficiency, reduced human error, faster production cycles, and better resource utilization.

Fourth, IIoT can also help with supply chain optimization by providing end-to-end visibility and transparency across the supply chain. By integrating data from suppliers, manufacturers, and distributors, organizations can track inventory levels, monitor shipping and logistics, and identify bottlenecks or inefficiencies.[15,16]

This is a big gain considering the recent supply chain crisis. IIoT enables better inventory management, improved coordination, and faster response times to changes in demand.[17] Ultimately, it creates a more efficient and agile supply chain.

continued →

The fifth benefit of IIoT integration is that it enhances worker safety and well-being. IIoT provides the ability to monitor environmental conditions, detect hazardous situations, and alert workers to potential risks. For example, sensors can monitor temperature, humidity, and air quality to ensure a safe working environment.

IIoT can also support wearable devices and location tracking to improve worker safety and emergency response in case of accidents or incidents.[18]

Another advantage is that IIoT improves product quality by enabling continuous monitoring and control of critical parameters during production. Real-time analysis allows for immediate detection of deviations or abnormalities, enabling timely adjustments and minimizing the production of defective goods.

Simply put, better visibility creates more consistency.

The final benefit is that IIoT provides cost reduction. It does so by optimizing resource utilization, streamlining processes, and reducing operational costs. As previously mentioned, IIoT also enables predictive maintenance, which minimizes the need for emergency repairs and reduces maintenance cost. ■

Understanding cloud connectivity

IIoT and cloud connectivity are two sides of the same coin. IIoT happens at the network's edge; it collects data and creates channels of communication to influence operations in real time. Eventually, much of that data ends up in the cloud for further processing.

Cloud connectivity enables devices, systems, and applications on the factory floor to connect and communicate with cloud-based resources and services over the internet. It facilitates data exchange, remote access, and centralized management of industrial processes and assets.

This typically involves transmitting data from the factory floor to cloud servers for storage, analysis, and integration with other enterprise systems. It allows real-time monitoring, data-driven decision-making, and utilization of advanced cloud-based tools and services to enhance operational efficiency and productivity.

Integrating IIoT with cloud connectivity provides many benefits. The most prevalent include data storage and analysis, scalability and flexibility, collaboration and integration, remote access and control, and cost savings.

First, the importance of data storage and analysis cannot be overstated. Cloud computing enables large-scale, long-term industrial data storage and retention in a secure and resilient environment.

Manufacturers can then use that data for big data analytics, machine learning, and other techniques that provide insights from vast amounts of historical and real-time data. This enables predictive maintenance, quality control, and process optimization.

The second benefit is scalability and flexibility. Cloud computing resources can be scaled up or down, instantly and on demand.[19] In addition to only paying for what they use, this means that manufacturers can easily accommodate growing data volumes and adapt to changing business requirements without investing in expensive on-premises infrastructure.

Third, cloud connectivity also facilitates collaboration and integration among various stakeholders. This is equally true for those within the organization and for external partners.

For instance, real-time data sharing, remote monitoring, and integration with enterprise systems such as enterprise resource planning (ERP) and customer relationship management (CRM) are all benefits of cloud connectivity on the plant floor.[20, 21] These integrations streamline operations and improve decision-making.

Fourth, don't forget about remote access and control. With cloud connectivity, anyone with an internet connection can access factory floor data from anywhere in the world. This is a big gain for remote workforces and for getting the most out of talent who may not be able to travel to every remote location when the need arises.

Remote access and control allow authorized personnel to monitor operations, troubleshoot issues, and make informed decisions—even when they aren't physically onsite. (Figure 3)

The fifth and final benefit is cost savings. On-premises infrastructure is expensive, both from a capital expenditure (CapEx) and operational expenditure (OpEx) standpoint. [22, 23] By working with a third-party cloud provider, manufacturers largely eliminate the CapEx side of the equation and significantly reduce the OpEx side.

By leveraging their cloud provider's infrastructure, manufacturers only pay for resources on subscription or usage-based models. The result is cost savings and improved resources utilization.

Public and private cloud options are two primary types of cloud connectivity for factory applications.

Public cloud connectivity is a common choice because it offloads much of the burden of setting up and running the

continued →

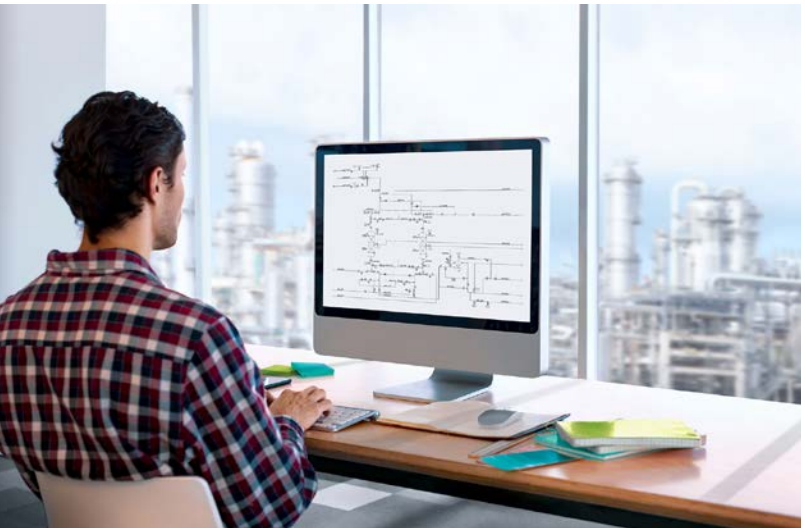

Figure 3: IIoT technology makes remote access and control possible, so personnel no longer have to be physically present at a site to access information or even troubleshoot problems.

IT infrastructure to another company. This route involves connecting factory floor devices and systems to public cloud platforms provided by third-party service providers such as Proficloud, Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP).

Public cloud platforms offer a range of services and resources, including data storage, analytics, machine learning, and application holistic. This solution provides cost-effective scalability, easy accessibility, and less overhead.

Private cloud connectivity, on the other hand, involves connecting those factory floor devices and systems to private infrastructure that's maintained and managed by the organization itself. Companies may choose to host private clouds either on-premises or in a dedicated data center.

While it lacks some of the advantages of public cloud, a private cloud offers greater control, security, and customization. That makes it the preferred solution in scenarios where data privacy, regulatory compliance, or specialized requirements are critical.

In some cases, **hybrid cloud connectivity** may be ideal because it combines the strengths of both. This means that organizations can keep sensitive data on a private cloud while still taking advantage of public cloud resources for scalability and access to specific services.

Ultimately, the choice between public and private cloud boils down to data security requirements, regulatory compliance, resource availability, and the organization's specific needs and priorities. ■

Key technologies for IIoT connectivity

IIoT is not a stand-alone technology. Networking and communication protocols are essential for enabling the interconnected factory, while cloud computing is important for storing and making use of the data that's collected and generated by IIoT devices.

Networking

Starting at the beginning, wireless networking technologies are at the crux of the matter because they put the I in IIoT. Manufacturers have a few options to choose from, and many deploy multiple networks to leverage their respective advantages and to provide redundancy.

The most common networking technologies for IIoT are Wireless Local Area Network (WLAN), public 5G, and private 5G networks. Each plays a crucial role in providing reliable, high-speed connectivity for a wide range of devices and applications.

WLAN, better known as Wi-Fi, is familiar and ubiquitous. In a manufacturing context, WLAN provides wireless connectivity within a limited area, such as a factory floor or warehouse. Devices can connect to a local network to access resources and services.

Just like Wi-Fi connectivity anywhere else, WLAN on the factory floor provides seamless networking for IIoT devices ranging from sensors and actuators to machinery and mobile devices.

These devices can communicate with each other over the network in real time, and they can also send and receive data from a centralized system, such as a supervisory control and data acquisition (SCADA) system.[24] This facilitates data collection, monitoring, and control.

WLAN also promotes flexibility and mobility. Workers and their mobile devices can access IIoT systems and their data from anywhere on the factory floor. This means that both workforces and processes gain an element of adaptability.

Scalability is another major benefit. Since manufacturers can easily scale a WLAN network to accommodate increasingly large numbers of devices, it's easy to expand an IIoT deployment without having to overhaul or upgrade the network. Organizations can also add additional access points to enhance coverage and capacity as needed.

Wi-Fi continues to be widely adopted in industrial applications largely due to the maturity of the technology and low cost per node. It also has a cost advantage over wired connections when manufacturers need to deploy IIoT devices across a large factory floor.

continued →

Finally, this networking technology is highly compatible. It's adopted by the world at large, meaning that it's highly standardized and it's hard to find a device that doesn't work with Wi-Fi. This is especially important for ensuring compatibility and integration between various devices and legacy systems in a manufacturing environment.

The next networking technology to highlight is public 5G networks, which are provided by telecommunication companies. Leveraging public 5G networks reduces overhead and lowers the cost of entry compared to Wi-Fi and private 5G networks.

The first main advantage of public 5G is enhanced bandwidth and throughput. These networks offer significantly higher bandwidth, with average download speeds ranging from 67.1 to 75.6 MBPS.[25, 26] That's about twice as much throughput as the previous generation of cellular connectivity.

Improved throughput enables IIoT devices to transmit large volumes of data in realtime, supporting applications like video streaming for computer vision, advanced analytics, and cloud-based services.[27]

Public 5G also boasts low latency and reliable communication. It's fast and resilient; just as with bandwidth, 5G offers significantly better latency numbers than previous generations.[28] This is a big advantage in industrial settings that support time-critical applications.

Real-time control, remote monitoring, and mission-critical applications become better and more reliable. This means that IIoT devices on public 5G can support applications like robotics, autonomous vehicles, and remote machine control. (Figure 4)

The final main benefit of public 5G is coverage and mobility. Since these networks cover wide areas, IIoT devices can connect in remote or challenging environments. As 5G rolls out to more rural locations, heavy industries have a lot to gain.[29] By tapping into a public 5G network, devices in a factory can maintain connectivity even while moving within the premises.

Similar to public 5G networks, private 5G networks offer many of the same benefits, with the main difference in the ownership and operations. Private 5G networks, deployed and managed either by the organizations themselves or by dedicated service providers, are becoming increasingly popular for IIoT deployments.[30]

The main reason private 5G networks are gaining popularity is dedicated connectivity. By tailoring the solution to the specific needs of the organization, private 5G networks offer reliable and predictable performance, ensuring consistent connectivity and data transfer for critical IIoT applications.

Second, we have network control and customization. These private networks give organizations complete control over their infrastructure, allowing manufacturers to select exactly how to prioritize variables like coverage, capacity, security, and quality of service. This enables manufacturers to optimize their network to meet their specific requirements.

Third, private networks offer enhanced security. Since they operate in a closed environment under the organization's control, private 5G networks add a layer of security compared to public 5G.

Figure 4: IIoT devices on public 5G can support applications like robotics, autonomous vehicles, and remote machine control.

This also enables organizations to implement further security measures, such as secure authentication, encryption, and access controls. For manufacturers that need to protect IIoT devices and data, private 5G is a good option.

Ultimately, by leveraging WLAN and 5G networks on the factory floor, organizations gain reliable, high-speed, and scalable connectivity for their IIoT deployments. When used in combination, WLAN provides local wireless connectivity within the factory premises, while 5G offers enhanced capabilities, including ultra-reliable and low-latency communication, massive device connectivity, high bandwidth, and network slicing.[31]

Putting these networking technologies together enables seamless communication, improved data exchange, and real-time control for IIoT applications.

In addition to the physical layer of communication, IIoT devices use communication protocols to talk to each other and the rest of the machinery on the factory floor. The most commonly used protocols for IIoT applications are Message Queuing Telemetry Transport (MQTT) and Open Platform Communication Unified Architecture.[32, 33]

continued →

Each has its own strengths and therefore serves a specific purpose based on the requirements of each individual application.

Starting with MQTT, that features a lightweight, publish/subscribe (pub/sub) messaging protocol that's designed for efficient communication between devices with limited bandwidth and processing capabilities.[34] The architecture consists of clients and brokers. A broker is the central hub that all clients connect to.[35] The broker manages the client connections, authentication, and distribution of messages. A client connects to a broker and publishes messages and/or subscribes to messages from other clients.

MQTT dominates both industrial and home IoT communications because it prioritizes low bandwidth consumption, low latency, and efficient communication. This makes it ideal for small devices with processing power and memory limitations.

That's why MQTT is commonly used in IIoT applications like telemetry, remote monitoring, and machine-to-machine (M2M) communication. It's well-suited for scenarios involving large numbers of devices that need to transmit periodic updates. For instance, devices may need to send sensor data to a central server or cloud platform for processing and analysis.

As previously mentioned, efficiency is one of the main draws of MQTT. This protocol minimizes network overhead by combining its lightweight nature with a publish-subscribe data flow—instead of sending out data indiscriminately, it only flows to subscribed devices. This makes MQTT efficient for constrained networks, reducing bandwidth and power consumption.

MQTT also has the benefit of customizable Quality of Service (QoS) levels that enable users to prioritize message delivery reliability and consistency according to individual application requirements. QoS levels range from "at most once" (QoS 0) to "at least once" (QoS 1) to "exactly once" (QoS 2).

This essentially defines how much confirmation is required to know that the message was received, in a somewhat similar vein to the differences between standard post, priority mail with tracking, and signature confirmation.

The last main advantage of MQTT is its inherent scalability. MQTT allows for large-scale IIoT deployments because numerous devices can efficiently publish and subscribe to different topics simultaneously. Since MQTT is so lightweight, it can handle large device populations without significant performance degradation.

The other communication protocol option is OPC UA, a standardized technology that's specifically designed for industrial automation and control systems. Whereas MQTT is more general-purpose, OPC UA is tailored to the demanding needs of manufacturing.

This enables OPC UA to offer seamless and secure data exchange between devices, machines, and software applications across different platforms. OPC UA also includes advanced features like data modeling and security, making it suitable for a wide range of IIoT use cases.

Because OPC UA was designed for interoperability between different industrial devices, systems, and software applications, it's most useful for systems integration across various components of an industrial ecosystem. Manufacturers use OPC UA to integrate sensors, actuators, SCADA systems, and enterprise-level software like ERP systems.

Another benefit of OPC UA is how the protocol handles data modeling. By providing a rich and extensible information modeling framework, OPC UA allows standardized representation of data and services.[36] A hierarchical structure for organizing information and support for complex data types means that OPC UA can enable comprehensive data representation and semantics.

Robust security mechanisms are another reason to choose OPC UA. Secure communication and data protection are especially important in IIoT applications. Because OPC UA supports encryption, authentication, and access control, it allows secure data transmission and prevents unauthorized access to critical systems and information.

As previously mentioned, the fact that OPC UA addresses the interoperability challenge is a big advantage. This standardized communication framework defines a common set of services, data models, and protocols, making it much faster, easier, and simpler to integrate different devices, systems, and platforms, regardless of vendor or legacy status.

The last main advantage of OPC UA is redundancy and reliability. By including features such as time synchronized networking (TSN), OPC UA ensures reliable data communication and system availability.[37] Building in redundancy, fault tolerance, and the ability to recover from communication failures makes the protocol suitable for mission-critical applications.

The choice between MQTT and OPC UA, therefore, depends on the specific requirements and characteristics of the IIoT application at hand.

MQTT is best suited for scenarios with low bandwidth, limited resources, and a large number of devices that transmit periodic updates. OPC UA, on the other hand, is ideal for industrial automation and control systems because it provides interoperability, advanced security, and data modeling capabilities.

continued →

Remember that, just as with 5G and WLAN, it's not a one-or-the-other decision; smart manufacturers lean into both in order to leverage their respective strengths and mitigate their weaknesses.

Computing

The final set of key technologies for IIoT connectivity on the factory floor are edge and cloud computing. The edge-cloud continuum refers to where the computing and data analysis actually happen.[38] Again, this isn't a one-or-the-other choice. Manufacturers can and should use the complementary capabilities of edge and cloud computing to handle the diverse requirements of industrial environments.

Edge computing refers to processing data and running applications at or near the network edge, closer to the data source or device.[39] By bringing computational resources and intelligence closer to where data is generated, edge computing reduces latency and enables real-time decision-making.

A common practice is to train a machine learning (ML) model in the cloud and then deploy it at the edge.

These are the key advantages of edge computing for IIoT applications.

First, real-time data processing allows for immediate data analysis either on the IIoT device itself or on a gateway device. This is particularly important for time-sensitive applications that require quick response times, such as real-time monitoring and control of industrial automation systems.

Another benefit is bandwidth optimization. Since data is processed locally, edge computing reduces the need to send large volumes of raw data to the cloud for analysis. Instead, it filters, aggregates, and pre-processes that data at the edge, sending only relevant or summarized information to the cloud.

This reduces the overall burden on the network by minimizing bandwidth usage, lowering latency, and reducing cloud infrastructure costs.

Edge computing also has offline capabilities, giving it an advantage in environments with intermittent or unreliable connectivity. This means that IIoT devices can continue operating and making decisions even if the connection to the cloud is disrupted. This ensures uninterrupted operation and minimizes downtime, even in challenging network conditions.

Enhancing data security and privacy is another reason to choose edge computing. Processing sensitive data locally minimizes the risk of transmitting it over the network. In turn, this reduces the exposure of critical data to potential cyber threats and helps organizations comply with data privacy regulations.

Finally, edge computing enables scalability in IIoT deployments by distributing computing across the network of edge devices. As the number of devices and data sources grows, manufacturers can add edge nodes to handle increased computational demands and to accommodate the system's growing scale.

The other side of the coin is cloud computing. This involves storing, managing, and processing data and applications on remote servers that are accessible over the internet. The cloud provides scalable and centralized computing infrastructure with extensive storage, high performance, and advanced analytical capabilities.

That's why data storage and analytics are the top reason to adopt cloud computing for IIoT use cases. Cloud data centers have vast storage capacity, enabling organizations to collect, aggregate, and store large volumes of IIoT data. This enables long-term data retention and historical trend analysis, and creates the ability to leverage big data analytics to gain insights and make informed decisions.[40]

Speaking of analytics, deploying machine learning and other advanced analytics is a great way to make use of the cloud's powerful computing resources. Organizations can process large datasets, perform complex analyses, and apply machine learning algorithms to extract valuable insights from their IIoT data. This enables predictive maintenance, anomaly detection, process optimization, and other data-driven decision-making.

Centralized management and control are also a benefit. By providing a centralized platform for managing and controlling IIoT deployments across multiple locations or facilities, cloud computing allows administrators to monitor, configure, update, and maintain devices, applications, and services. This provides visibility and control over the entire IIoT ecosystem.

The cloud also facilitates collaboration and integration by enabling real-time data sharing, collaboration among stakeholders, and integration with other enterprise systems like ERP and CRM systems. The end result is a seamless information flow and improved operational efficiency.

Finally, the cloud is also well-known for scalability and elasticity. There's virtually no limit to how much a cloud platform can scale. And it's easy to go up and down—elasticity allows organizations to add or subtract resources based on demand. This eliminates the need to invest in and manage on-premises infrastructure, enabling cost savings and flexibility in resource application.

Don't forget that edge and cloud computing are most powerful when combined. Together, they provide a holistic solution for IIoT application.

continued →

Edge computing handles the real-time processing, low-latency decision-making, and local data management. Meanwhile, cloud computing provides centralized storage, advanced analytics, and scalable infrastructure for long-term data analysis, collaboration, and system management. ■

Best practices for implementing IIoT connectivity

Whether you're just starting to build a pilot program or you want to build on a successful proof-of-concept to scale out your IIoT deployment across your operations, you'll need to follow a road map.

Begin by identifying use cases or areas where IIoT can bring value to your factory floor operations. Build out a business case with clear objectives, operational challenges, and the potential benefits of implementing the IIoT solution. Clearly defined goals and expected outcomes will guide the entire implementation process.

The next step is to evaluate existing infrastructure, including network capabilities, hardware, and software systems. Identify any gaps or limitations that must be addressed to support IIoT connectivity. Consider factors such as connectivity options, data storage and processing capabilities, scalability, and compatibility.

Third, select the right technology. Find appropriate IIoT technologies that align with your use cases and infrastructure requirements. This involves selecting suitable sensors, devices, communication protocols, and data management platforms. Important factors include connectivity options (WLAN, 5G, or wired connection), data transfer protocols, real-time requirements, and integration capabilities with existing systems.

Next, address security concerns early and often. Instead of waiting until after implementation to bolt on security, design security from the ground up to protect IIoT systems and data from cyber threats. This means implementing secure communication protocols, encryption mechanisms, access controls, and authentication.

Build processes for regularly updating and patching software systems, conducting security audits, and ensuring compliance with relevant security standards and regulations.

After that, ensure interoperability by making certain that IIoT devices can seamlessly communicate and share data with each other and existing systems and applications. Open standards like OPC UA can help facilitate integration across different devices and platforms. Application Programming Interfaces (APIs) and middleware solutions can also enable data exchange and interoperability between systems.[41]

By following these best practices, you'll successfully implement IIoT on the factory floor. The end results will be improved operational efficiency, enhanced decision-making, and optimized processes. ■

Conclusion

Start today on tomorrow's smart factory

Manufacturing practices continue to evolve.

Just as the invention of the steam engine ushered in the industrial revolution in the 1830s, Industry 4.0 technologies like IIoT and cloud computing represent an equally seismic shift in how goods are produced.[42]

Now, just as then, there will be challenges. Some workers will need to learn new ways of working, while their employers will simultaneously struggle to find the talent needed for new roles being created.

As discussed in the section on workforce challenges, upskilling and reskilling will be absolutely necessary for a successful transition. The companies that come out ahead will take a proactive approach to both hiring upcoming talent and training their existing workforce.

At the same time, management needs to begin building proofs-of-concept that will enable it to craft business plans and make smart bets with it's investment. There are tons of Industry 4.0 technologies on the market, each with its own value proposition; it's up to corporate leaders to figure out where to put the smart money to maximize their ROI.

Executives can only do so by getting ahead of the curve. Waiting minimizes their ability to start small, run experiments, and figure out what works and what doesn't, given each business's set of unique circumstances.

Engineers will also need to take on a big-picture perspective. The word of the day is integration. IIoT is like having eyes and ears throughout the factory, but, without layers of intelligence that put everything together, we risk a disjointed operation.

The assembly line is becoming even more tightly integrated, both within itself and with the broader enterprise tech stack. Technical professionals need to understand both the business requirements and how to translate them into an actionable solution.

continued →

As a corollary, manufacturers will need to bridge the gap between OT and IT teams as their worlds begin to blur together. Smart manufacturing is just that: data and analysis applied to physical machines performing physical tasks. Organizations need to start breaking down silos if they want a successful transition.

Then there's the security aspect. Safety and security have always been a concern for heavy industries, but now there's also the necessity to guard against constantly evolving cyber threats.

This is another case where waiting and being reactive are not an option. By the time the network becomes infected with ransomware or malware, the damage is done. Only a proactive approach can prevent these worst-case scenarios.

We understand that it's a lot. And there are many voices clamoring for your attention, often with different opinions and approaches. That's why it's so important to work with a partner that you can trust.

Phoenix Contact has remained the leading company in industrial automation for over 100 years. We've navigated through changing conditions before, and we're continuing to pioneer new technologies and methodologies as we help our manufacturing partners transition to the modern smart factory.

We're here for you. If you need help with cloud or IIoT connectivity, be sure to follow me on LinkedIn or ask us a question today. ■

About Phoenix Contact

Phoenix Contact is a global market leader based in Germany. Phoenix Contact produces future-oriented components, systems, and solutions for electrical controls, networking, and automation. With a worldwide network reaching across more than 100 countries, and with over 22,000 employees, Phoenix Contact maintains close relationships with its customers, which is essential for shared success. The company's wide variety of products makes it easy for engineers to implement the latest technology in various applications and industries. Phoenix Contact focuses on the fields of energy, infrastructure, process, and factory automation.

For more information about Phoenix Contact or its products, visit **www.phoenixcontact.com**, call technical service at **800-322-3225**, or email **us-info@phoenixcontact.com**.

References

1. "What Are Industry 4.0, the Fourth Industrial Revolution, and 4IR?" McKinsey & Company, 17 Aug. 2022, www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-industry-4-0-the-fourth-industrial-revolution-and-4ir
2. "A manufacturer's guide to scaling Industrial IoT." McKinsey & Company, 5 Feb. 2021, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/a-manufacturers-guide-to-generating-value-at-scale-with-industrial-iot
3. Chitkara, Raman, and Rob Mesirow. "The Industrial Internet of Things." PwC, https://www.pwc.com/gx/en/technology/pdf/industrial-internet-of-things.pdf
4. Ellingrud, Kweilin, Rahul Gupta, and Julian Salguero. "Building the vital skills for the future of work in operations." McKinsey & Company, 20 Aug. 2020, https://www.mckinsey.com/capabilities/operations/our-insights/building-the-vital-skills-for-the-future-of-work-in-operations
5. "Advanced Manufacturing Sciences Institute." Metropolitan State University of Denver, https://www.msudenver.edu/advanced-manufacturing/
6. "Industrial Internet of Things (II0T)." University of Michigan. Michigan Online, https://online.umich.edu/courses/industrial-internet-of-things/
7. Serror, Martin, and Sacha Hack, Martin Henze, Marko Schuba, and Klaus Wehrle. "Challenges and Opportunities in Securing the Industrial Internet of Things." arXiv.org. Cornell University, https://arxiv.org/pdf/2111.11714.pdf
8. "CIA Triad." Fortinet, https://www.fortinet.com/resources/cyberglossary/cia-triad
9. McQuade, Mike. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." Wired, 22 Aug. 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
10. Sanger, David E., Clifford Krauss, and Nicole Perlroth. "Cyberattack Forces a Shutdown of a Top U.S. Pipeline." New York Times. Updated 13 May, 2021, https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html
11. "General Data Protection Regulation." Intersoft Consulting, https://gdpr-info.eu/
12. Frankenfield, Jake. "What Is Personally Identifiable Information (PII)? Types and Examples." Investopedia, Updated 2 Nov. 2023, https://www.investopedia.com/terms/p/personally-identifiable-information-pii.asp
13. Bhamidipaty, Anuradha, and Dhaval Patel, Shuxin Lin, Srideepika Jayaraman, Giridhar Ganapavarapu. "What is anomaly detection?" IBM. 15 Nov. 2021, https://developer.ibm.com/learningpaths/get-started-anomaly-detection-api/what-is-anomaly-detection/
14. "What is predictive maintenance?" IBM, https://www.ibm.com/topics/predictive-maintenance
15. Wendt, Eric. "Strengthening the supply chain with IIoT technology." Control Engineering, 6 April 2022, https://www.controleng.com/articles/strengthening-the-supply-chain-with-iiot-technology/
16. "Using IoT Sensors to Improve Productivity in Manufacturing." DataBlaze, https://datablaze.com/news/using-iot-sensors-to-improve-productivity-in-manufacturing/
17. Gamio, Lazaro, and Peter S. Goodman. "How the Supply Chain Crisis Unfolded." New York Times. 5 Dec. 2021, https://www.nytimes.com/interactive/2021/12/05/business/economy/supply-chain.html
18. "Industry 4.0 Evolves: The Wearable Industrial Internet of Things." The Thales Group. 30 Nov. 2020, https://www.thalesgroup.com/en/worldwide-digital-identity-and-security/iot/magazine/industry-40-evolves-wearable-industrial
19. "What Is Cloud Scalability?" VMWare by Broadcom, https://www.vmware.com/topics/glossary/content/cloud-scalability.html
20. The Investopedia Team, "Enterprise Resource Planning (ERP): Meaning, Components, and Examples." Investopedia, 28 March 2023, https://www.investopedia.com/terms/e/erp.asp
21. Rudder, Alana, and Kelly Main. "What Is CRM? The Ultimate Guide (2023)." Forbes Advisor, Forbes, 19 Aug. 2022, https://www.forbes.com/advisor/business/what-is-crm/
22. Fernando, Jason, "Capital Expenditure (CapEX) Definition, Formula, and Examples." Investopedia, Updated 30 Oct. 2023, https://www.investopedia.com/terms/c/capitalexpenditure.asp
23. Ross, Sean. "CapEx vs. OpEx: What's the Difference?" Investopedia, Updated Dec. 4 2023, https://www.investopedia.com/ask/answers/112814/whats-difference-between-capital-expenditures-capex-and-operational-expenditures-opex.asp
24. Loshin, Peter. "SCADA (supervisory control and data acquisition)." TechTarget, updated Dec. 2021, https://www.techtarget.com/whatis/definition/SCADA-supervisory-control-and-data-acquisition
25. Fisher, Tim. "What Is Bandwidth? Definition, Meaning, and How Much You Need." LifeWire, updated 21 Oct. 2023. https://www.lifewire.com/what-is-bandwidth-2625809
26. Tom's Guide Staff. "5G speed: 5G vs. 4G performance compared." Tom's Guide, 1 June 2021, https://www.tomsguide.com/features/5g-vs-4g
27. "What is computer vision?" IBM, https://www.ibm.com/topics/computer-vision
28. Shankland, Stephen, and Shara Tibken. "5G Latency: Why Speeding Up Networks Matters." CNET, 1 July 2021, https://www.cnet.com/tech/mobile/5g-latency-why-speeding-up-networks-matters-faq/
29. Salter, Jim. "5G in rural areas bridges a gap that 4G doesn't, especially low- and mid-band." ARS Technica, 14 Sept. 2020, https://arstechnica.com/features/2020/09/5g-03-rural/
30. Control Engineering Europe, "Connecting industrial applications to a private 5G network." Control Engineering, 19 Oct. 2020, https://www.controleng.com/articles/connecting-industrial-applications-to-a-private-5g-network/
31. Burke, John. "Network slicing." TechTarget, https://www.techtarget.com/whatis/definition/network-slicing
32. "MQTT: The Standard for IoT Messaging." MQTT, https://mqtt.org/
33. "Unified Architecture." OPC Foundation, https://opcfoundation.org/about/opc-technologies/opc-ua/
34. Wickramasinghe, Shanika. "What Is Pub/Sub? Publish/Subscribe Messaging Explained." BMC, 26 July 2021, https://www.bmc.com/blogs/pub-sub-publish-subscribe/
35. HiveMQ Team. "MQTT Essentials: Part 3." HiveMQ, updated 6 June 2023, https://www.hivemq.com/blog/mqtt-essentials-part-3-client-broker-connection-establishment/
36. "Unified Architecture." OPC Foundation, Dec. 2017, https://opcfoundation.org/about/opc-technologies/opc-ua/
37. "Welcome to OPC UA over TSN: A New Frontier in Ethernet Communications." OPC Foundation, https://opcconnect.opcfoundation.org/2017/12/opc-ua-over-tsn-a-new-frontier-in-ethernet-communications/
38. "The edge-cloud continuum is fueled by flexibility and insight." Deloitte On Cloud podcast, https://www2.deloitte.com/us/en/pages/consulting/articles/cloud-to-edge-success-fueled-by-flexibility-insight-and-information-for-cloud-professionals-podcast-with-aws.html
39. "What Is the Network Edge?" Fortinet, https://www.fortinet.com/resources/cyberglossary/network-edge
40. "Big data analytics." IBM, https://www.ibm.com/analytics/big-data-analytics
41. "What is middleware?" IBM, https://www.ibm.com/topics/middleware
42. History.com editors, "Industrial Revolution." History.com, updated 27 March 2023, https://www.history.com/topics/industrial-revolution/industrial-revolution#when-was-the-industrial-revolution

All sources accessed November 30, 2023.