BURNS McDONNELL

WHITE PAPER

Manage Facilities More Efficiently Through the Industrial Internet of Things

By Anagha Dalal and Mandar Rangnekar

Investment in the Industrial Internet of Things (IIoT) can provide the means to correlate supply and demand with plant capabilities at various locations. Additionally, it can improve inventory planning, optimize the scheduling of field services and enable a quick response to upcoming market opportunities.

Information technology (IT) has changed the way organizations function, with large numbers of smart gadgets continuously connected to the internet. These gadgets constitute what is known as the Internet of Things (IoT), and when extended to manufacturing and production, this is known as Industrial Internet of Things, or IIoT. The things in the IIoT are intelligent machines that share data using advanced communication technologies for more reliable, efficient and safe operation of plants. Most of the devices are connected to the network to allow continuous monitoring and control. IIoT has the potential to unleash benefits by providing information that can be used for increasing plant availability, resulting in operating the plant near the threshold design parameters and minimizing downtime. While technology is no longer a constraint, the means of implementing it for use in the industry can be challenging.

The IIoT is a trending topic in the process and automation industry. This technology has the potential to help the industry tap into capacity and capabilities that exist in plants but historically have gone unutilized. This paper focuses on the fundamentals, implementation and challenges of IIoT. IIoT usually refers to interconnected sensors, instruments and other devices in an industrial setting. This connectivity enables remote access and monitoring, and it facilitates data acquisition, collection, exchange and analysis from different sources. This has enormous potential for improving productivity and efficiency. IIoT solutions are characterized by their low cost and fast implementation.

For example, a supplier needs to publish new functionalities on the human-machine interface (HMI) for a client. However, when a machine is delivered and the client uses it for daily operations, it might require extra functionality to simplify the job further. An expansion of the control panel with a new function, such as an on/off switch or a percentage counter for the pump, can easily be fixed by the programmer. But the HMI software needs to be updated and tested to launch this new functionality. HMI software updates can easily be applied remotely via secure network access. Using a virtual network connection (VNC), HMI functionality in the IIoT platform or on a mobile device can be viewed and tested.

IIoT can also be useful in predicting maintenance and analyzing which part will need to be replaced. Sometimes it is easy to predict when a machine requires maintenance, for example, when the degradation rate for a machine is identified based on production hours or runtime. In these scenarios, it makes sense to implement predictive maintenance by using the variables (counters) of the programmable logic controller (PLC) software and logging this data to the cloud. Vendors can access the data, analyze the machine behavior and alert the client. Clients can also visualize the machine's performance on the dashboard and get an email reminder when maintenance is due.

On-site machine maintenance visits are more effective when the technician is aware of the faults before reaching the site. The right spare parts can be identified in advance by analyzing potential problems using remote access and the online diagnostics tool of the device's web server.

IoT Versus IIoT

IoT applications are deployed on devices in a range of industries, including agriculture, healthcare and consumer goods, as well as for municipalities. IoT devices include smart appliances, fitness bands and other applications that alert users in emergency situations when something goes amiss.

IIoT applications, on the other hand, connect machines and devices in industries such as oil and gas, utilities and manufacturing. System failures and downtime in IIoT deployments can result in high-risk or even life-threatening situations. IIoT applications are also more focused on improving efficiency and health and safety, versus the user-centric nature of IoT applications.

OT, IT and IIoT in Process-Driven Industries

The connection of all process parameters in a plant's control system forms the backbone of operational technology (OT). Implementing OT capabilities on Ethernet, local area network (LAN) or wide area network (WAN) to share plant information for further optimization formalizes the concept of IT for the industry.

IIoT is a combination of OT and IT, bringing the process parameter information to a common platform to share relevant data with systems in real time. In process-driven industries, these inputs vary from the data of known tagged plant devices to information from untagged sensors that is available but remains unutilized. The innovations in hardware and their connectivity with communication networks in recent decades have made this a reality. The signal transmission from sensors has migrated from conventional 4-20 milliampere (mA) current signals to digital signals such as highway addressable remote transducer (HART), foundation fieldbus and wireless. These signals not only share details of process parameters but also provide diagnostic information about the sensor. Bringing this valuable information onto the network provides better insight into these individual components and improves the overall health of the plant.

With smart devices in place, critical processes can share ample information with the control systems on an open platform. A structured approach to scrutinize and analyze this data is required to gain real insight. IIoT predominantly shares plant data with original equipment manufacturers and analysis vendors on a secured network to get their opinions. The data is analyzed either locally or remotely to extract meaningful and actionable information for field operations.

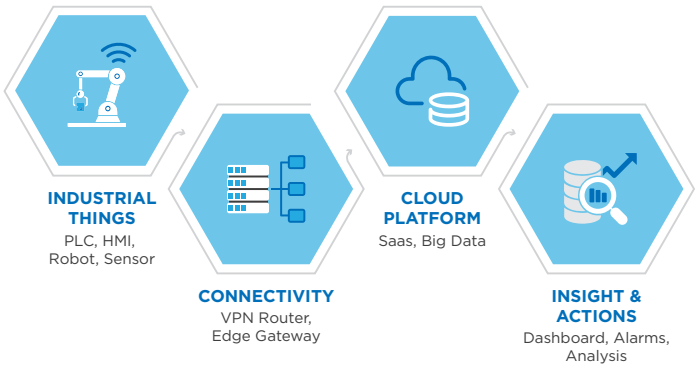

***Figure 1:** Essentials of IIoT. Source: https://www.ixon.cloud/knowledge-hub/7-practical-applications-of-iiot-in-industrial-automation.*

Basic Architecture of IIoT

OT network: This network comprises field sensors integrated with the control system data highway. Supervisory control is implemented via operator stations on the data highway.

IT network: This consists of the enterprise network automatically collecting information from various plants and facilities and making it available on an open platform for further analysis.

Cloud: Industrial data is stored on the cloud and securely shared with third parties. This provides a standardized platform, allowing third parties to develop tools and applications independently. Smartphone apps connecting to the cloud can enable operators to read alerts, analyze data and take corrective action instantaneously.

Service provider network: This allows third parties to interpret and analyze data, deriving actionable information for the end user.

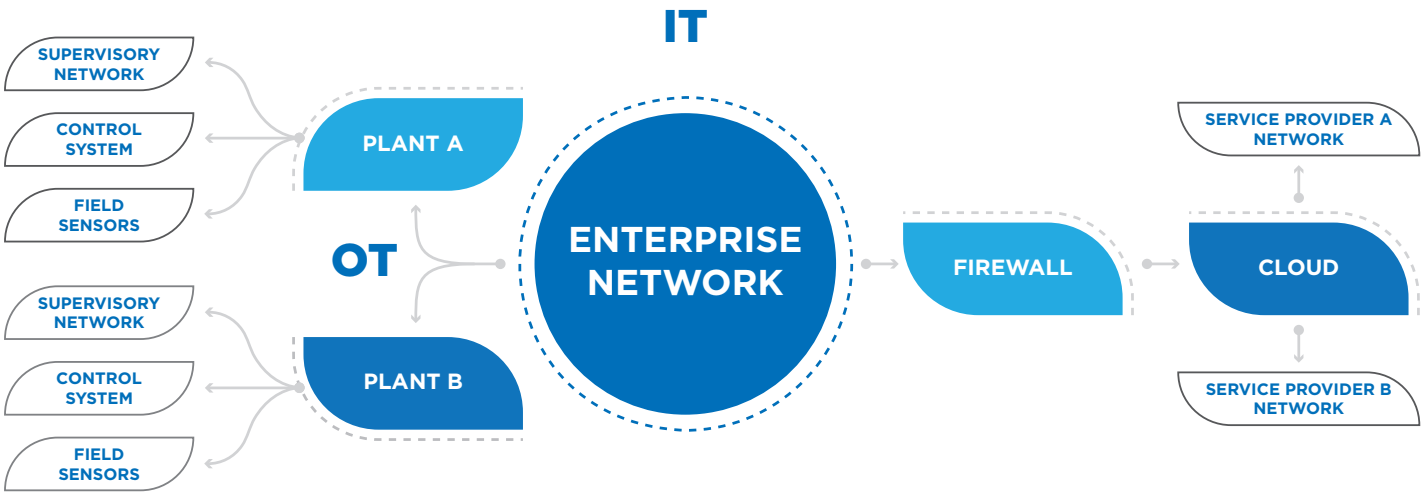

***Figure 2:** Basic Architecture of IIoT.*

Evolution of Control Systems

IIoT is primarily an extension of the existing digital plant network (OT and IT). Data is sent to third-party specialists for analysis, providing valuable information for predictive control instead of reactive control. In other words, IIoT is an evolution of a distributed control system that allows for a higher degree of automation by using cloud computing to refine and optimize the process controls.

IIoT is transformational — changing the way industrial companies operate day to day. Examples could include enabling predictive analytics to detect corrosion inside a refinery pipe, providing real-time production data to uncover additional capacity in a plant, or accelerating new product development by feeding operations and service data back into the product design cycle. IIoT and the software solutions powered by it drive powerful business outcomes.

By combining machine-to-machine communication with industrial big data analytics, IIoT is driving unprecedented levels of efficiency, productivity and performance. And as a result, industrial companies are experiencing transformative operational and financial benefits.

The Need for IIoT

When major plant equipment breaks down, significant productivity is lost. The conventional way to address this is to have scheduled maintenance. However, what if the equipment malfunctions before this? It will lead to productivity loss. On the other hand, what if the equipment does not require maintenance? Then the time and efforts involved could be used for more productive work. This would assist in reducing downtime and saving money.

Process-driven industries already have a form of predictive maintenance, driven by integrated smart devices connected to the control system. However, the data required to adjust the predictive maintenance with machine behavior and assess the necessity of maintenance can be acquired with IIoT.

When the enterprise network observes repetitive faults in a similar process across various plants, IIoT shares that information with the service provider. The service provider can then work with the end user to perform a root cause analysis for critical faults, upgrade its own system and share lessons learned with the end user, thus enabling continual improvement. The shorter response time for similar issues and lower maintenance cycles improves plant operability.

Imagine if control of an offshore oil and gas platform gets completely digitized. Multiple providers have developed solutions to digitize operation of an oil and gas platform by making a digital twin. It consists of two main components: a process twin and a plant twin.

The process twin is a digital replica of the process and automation system that enables testing of the process and control, safety logic and operating procedures. The plant twin is a smart 3D model that provides access to equipment, carrying out real-time operations and maintenance by operating robotic arms on the platform from remote control rooms.

This digitization can reduce capital and operating expenses, shorten project development cycles, minimize interfacing risk and decrease offshore labor requirements. Accordingly, the digitization can bring down production costs significantly.

Relevant IoT Standards

Standard development organizations like the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) have published their first editions of some standards to set the ground rules for data integration and its safety. These include:

ISO/IEC 20924: IoT — Vocabulary: This standard provides a definition of IoT along with a set of terms and definitions. This document is a terminology foundation for the IoT.

ISO/IEC 30141: IoT — Reference Architecture (IoT RA): This document specifies a general IoT reference architecture in terms of defining system characteristics, a conceptual model (CM), a reference model (RM) and architecture views. The reference architecture includes:

- The generic characteristics of IoT systems.
- The CM, describing the key concepts characterizing an IoT system.
- The RM, providing the overall structure of the elements of the architecture.
- A set of reference architecture views, describing the architecture from several perspectives.

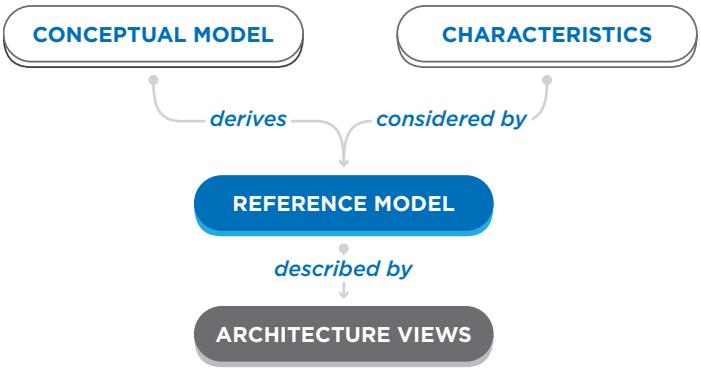

***Figure 3:** IoT Reference Architecture, Source: ISO/IEC 30141, 2018 edition.*

In short, the IoT RA provides guidance to the architect developing an IoT system and aims to give a better understanding of IoT systems to the stakeholders of such systems, including device manufacturers, application developers, customers and users.

Challenges in Implementing IIoT

The manufacturing industry will have to overcome several challenges before IIoT systems are widely adopted. These include building up the standards around IIoT, high investment, connectivity, cybersecurity, data analysis and workforce adoption of a new set of skills.

Standardization

Industries need standards to allow smart devices, machines and other assets to interact with each other in predictable fashion. This goes beyond the normal communication protocols and involves generation of standard semantics and operating procedures, which will allow smart devices to discover and interact with each other.

High Investment

The upfront cost of updating from older products to IIoT-enabled products is very high. Among the main purposes of IIoT is to improve manufacturing efficiencies — and reduce the maintenance and financial losses attributed to equipment failures — through better asset management and productivity gains. Along with product development, support of resources specializing in IIoT is critical.

Connectivity

One of the main requirements for adopting IIoT is having reliable and strong data networks. Studies show that in 85% of factories worldwide, machines are not connected or are unable to collect or provide data and transmit it back. One of the main reasons is legacy devices have long life spans, do not support data-driven tools and offer few connectivity options. Also, because high-speed internet still is not consistently available everywhere, connectivity remains a significant challenge even where newer devices are implemented.

Cybersecurity

Bringing industrial data onto an open communication platform makes it more susceptible to cyberattacks.

The process plant networks, also known as supervisory networks, are primarily designed for integrated functionality and safe performance within the plant hierarchy. This design is based on the control system vendor's proprietary software, which may require special skill sets. This supervisory network is generally set up using the enterprise network. When this is moved to the cloud, plant data is exposed to an external network, thus making critical information more vulnerable.

The IEC 62443 standard covers cybersecurity through the following sections:

- **Section 1 – General:** Defines concepts and models.
- **Section 2 – Policies:** Defines security management and patch management.
- **Section 3 – System:** Defines security technology and risk assessment.
- **Section 4 – Component:** Defines product development and technical security requirements.

The risk of cyberattacks can be mitigated by implementing the following:

- **Network security parameters:** Use of firewalls confirms isolation between the plant network and external network, as well as between third-party systems within the plant.
- **Hardware locks:** Integration of user ID and password into dedicated workstations limits access to authorized operators only.
- **Account management:** Planned, regular changes of user IDs and passwords for better security.
- **Updates:** Regular security updates in the form of patches keep systems armed against attacks by new viruses.
- **Backup:** An efficient backup and recovery plan allows operators to revert the system to a healthy state.
- **Audits:** Consistent security audits detect any unwanted events and assist in proactively mitigating issues.

Data Analysis

A main method for implementing IIoT solutions in manufacturing is to expand manufacturing facilities with tools for data acquisition, analysis and visualization. The sensory and control equipment connected to a SCADA system generates large amount of raw data, which needs to be analyzed to gain insights.

Analyzing this large amount of data is important to gain efficiencies. In many organizations, this valuable data is not collected or stored in a structured and efficient manner. So, it is important for organizations to hire data analysts with the required skills.

Workforce Adoption

The skill sets required to design and operate an IIoT-based system are very different from those needed to run a traditional automation system. A significant amount of retraining will be required for existing operators and maintenance staff to manage such systems.

Conclusion

The evolving concept of IIoT is creating a new turning point for many industries. Consider oil and gas, for example: The possibilities of analyzing captured data and utilizing the findings will benefit upstream (well site exploration and production), midstream (transportation pipelines) and downstream (onshore processing) sectors. Plants equipped with smart devices can obtain the maximum advantage from their existing digital infrastructure.

Investments in IIoT are expected to provide the means to correlate supply and demand with plant capabilities at various locations, improve inventory planning, optimize the scheduling of field services, and enable a quick response to upcoming market opportunities.

Technology suppliers, engineering contractors and end users all have roles to play in understanding the concept of IIoT. Even though implementation of IIoT will be driven by the end user, it is critical that any detailed engineering contractor has sufficient knowledge to execute the engineering design in accordance with the facility requirements.

Some of the key tasks in implementing IIoT will include finalizing the concept, designing architecture, employing open integration protocols, defining methods to consolidate data, mining data, assigning measures to mitigate risks, and identifying the flow of work across the organization.

The IIoT can bring about a steep change in operational activities and business strategies. However, security and maintaining the privacy of industrial networks are prime concerns and will continue to remain so. Unless regulatory standards are put in place and the means to minimize security breaches are established, industries will be challenged to gain all the possible advantages from IIoT.

About Burns & McDonnell

Burns & McDonnell is a family of companies bringing together an unmatched team of engineers, construction professionals, architects, planners, technologists and scientists to design and build our critical infrastructure. With an integrated construction and design mindset, we offer full-service capabilities. Founded in 1898 and working from dozens of offices globally, Burns & McDonnell is 100% employee-owned. For more information, visit **burnsmcd.com**.

23683-0122