Five Key Elements for Effective IIoT Implementation

Assessing Existing Infrastructure and Requirements

White Paper

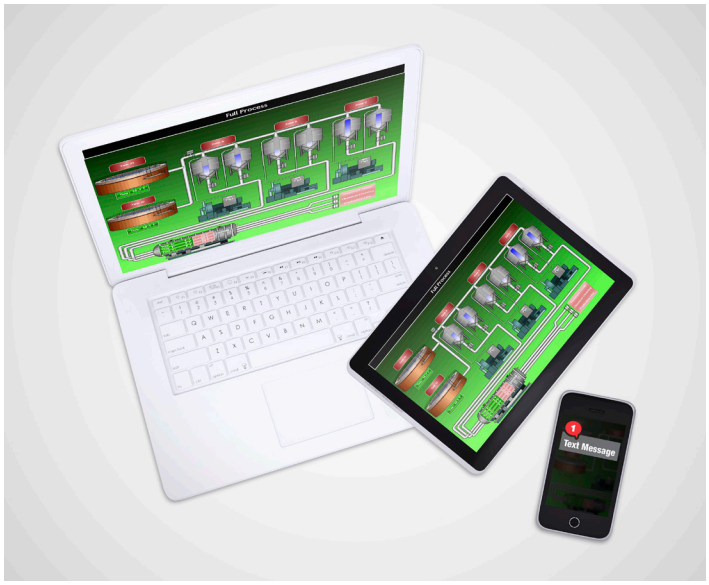
Five Key Elements for Effective IIoT Implementation

Industrial automation exists within a broader technological framework and has benefitted from advances in industrial networking and mobile computing. The combination of these technologies is helping to make the vision of concepts like the “Connected Factory”, “Industry 4.0” and the Industrial Internet of Things (IIoT) a reality. Often however, the proliferation of competing concepts can lead to confusion and leave some questioning how to begin practical implementation. After defining these concepts, this white paper will examine key elements organizations should consider when devising an effective implementation strategy and also explore the benefits that will result from connecting, monitoring and controlling operations.

Table of Contents

Introduction

Many technological advances have been made over the past two decades. Of these, industrial networking and mobile computing continue to impact manufacturing and industrial environments. These are the technologies that are helping to make the vision of concepts like the “Connected Factory”, “Industry 4.0” and Industrial Internet of Things (IIoT) a reality for manufacturers and organizations around the world. But how do these concepts differ? After defining these concepts, this white paper will examine key elements organizations should consider when devising an effective implementation strategy and also explore the benefits that will result from connecting, monitoring and controlling operations.



Concept Definition

What is the Connected Factory?

The Connected Factory is the vision of a manufacturing environment where every machine is able to communicate with all other machines and devices across the plant floor and other remote locations. The purpose of the Connected Factory is to connect, monitor and control virtually anything, anywhere to drive operational productivity and profitability.

What is Industry 4.0?

According to Wikipedia, Industry 4.0 is a “collective term for technologies and concepts of value chain organization.” This term originated from a German-government initiative that refers to the fourth industrial revolution, based upon the dynamic optimization of production resources within and between highly-connected factories.

What is the IIoT?

Similar to the Connected Factory and Industry 4.0, IIoT will mean that organizations will be able to connect many different devices, including older equipment, and get them to “talk” with each other in a way that they could not before. By gathering data from both new and legacy devices, organizations can use that data to improve efficiency and gain a competitive advantage.

“The purpose of the Connected Factory is to connect, monitor and control virtually anything, anywhere.”

Devise an Effective Implementation Strategy

Many of today's organizations are eager to implement Connected Factory, Industry 4.0 and/or IIoT concepts to realize benefits, such as reduced operational costs and better visibility and control. While it is, however, unrealistic and cost-prohibitive for most organizations to construct green-field facilities or "rip-and-replace" legacy equipment, many solutions utilize existing equipment and allow components to be strategically deployed to extend monitoring and control capabilities without impacting day-to-day operations. When updating a facility, it is important that expectations be set early. Despite the vision of an IP address for every piece of equipment in a network, the reality is end users will not be able to log into every panel meter, water pump and drive from mobile devices. Bringing a facility into the 21st century involves several core fundamentals to help ensure a smooth transition and provide the ability to access, monitor and control information from anywhere.

The first step when devising an effective implementation strategy should revolve around an organization's operational environment and the devices, applications and processes that make it up. Before plans are put into action, organizations should consider the following five key elements:

1. Legacy Equipment

Take inventory of the devices and equipment across the network. How old are they? Do they need to be replaced or upgraded? Is legacy equipment going to be able to communicate with newer equipment? How much time and money will this take? What cost-effective solutions can address this infrastructure?

2. Protocols/Communication

Along with the equipment, what protocols are being used by networked devices? How many are in use? Do they need to be converted in order to get the devices to communicate with others in the same environment? What type of media cabling is being used across locations? Fiber-optic cable? Serial (RS-232/422/485)? USB? Copper?

3. Location/Environment

Where is the facility located? If equipment is in a remote location, can each device be monitored via cellular networks? Are 4G/LTE or 3G networks available to reach the site? If not, are broadband or fiber-based networks available? Also, within the building itself, what is the overall environment? Hot and dusty, or at a controlled temperature? Lots of vibration? Are there flammable gases? Is industrial-grade equipment that is designed with wide environmental ratings and industry certifications being used?

4. Security

According to a recent Business Insider Intelligence survey, 39% of executive respondents indicated that privacy and security are the most significant barriers to IoT investment. Security was the most commonly cited concern among respondents. While this survey applies to all items in IoT, security should be an important concern for IIoT as well. How can sensitive data be protected when it is collected and transferred? What security measures are in place for the systems that collect, monitor, process and store IIoT data? Are there any regulations regarding the protection of data and information?

5. Staff

As more technology-based devices are added to the network, is the right IT staff on hand? Are other employees who are tech savvy available to help with installation and monitoring? Is software or remote monitoring needed to keep tabs on devices in other locations?

Once these key elements are assessed and questions answered, organizations should take steps to:

- Enable communication between devices
- Ensure operational efficiencies across the infrastructure
- Provide a secure platform for device communication

Enable Communication Between Devices

Drives, sensors, PLCs, panel meters and other automation equipment are built to last years – even decades. Trouble is they often communicate via proprietary protocols that commonly use RS-232/422/485 serial cables. While these serial protocols are efficient and were often written for a specific application, many of these applications never included 24/7 monitoring across TCP/IP networks. In order to bring these devices into the Connected Factory, Industry 4.0 and/or IIoT paradigm, an organization's engineers must first ensure that the devices can communicate with the other equipment on the factory floor. Companies looking to connect devices from disparate manufacturers can now choose advanced HMIs, protocol converters and other automation products that natively speak different protocols. These industrial products enable devices to communicate regardless of physical medium and offer industrial fluency and multi-protocol support.

Ensure Operational Efficiencies Across the Infrastructure

Operational efficiencies can be accomplished in a number of ways, one of which is using data collected from monitoring points along a manufacturing line to minimize waste and downtime. As technology continues to improve, these status points will include an increased volume of information from a wider range of sources. Managed Ethernet switches will be able to report on the flow of data throughout the facility in the same way that sensors on assembly lines can report a product's status on a production line. This expanded collection of operational data enables organizations to make data actionable by using visual management solutions to collect, record and display critical Key Performance Indicator (KPI) and Andon messages. Displaying this critical performance data in real time helps to drive productivity and increase throughput. This concept is not limited to connecting, communicating and monitoring within an organization. This concept can also be extended to include the supply and distribution chain to present a comprehensive view of the entire operation.

Provide a Secure Platform for Device Communication

Security has traditionally meant physical isolation of automation equipment and enterprise networks. If nothing is connected to automation equipment, the threat of security breaches is fairly low. Connection-free facilities are few and far between as more organizations continue to expand their enterprise networks into factory settings. As organizations embrace this new reality, security should be addressed through careful network planning and use of IP address best practices. Routers can be deployed within a network to limit network traffic to specific types of traffic or to specific users, minimizing the risk of a cyber-attack. Another tactic is the implementation of NAT (Network Address Translation). NAT is a technique that obscures devices on a network from inbound access, but doesn't affect traffic on a network. Finally, using VPNs or tunneling appliances also makes factory-to-factory, supply chain-to-factory, or factory-to-distributor communication secure by creating virtual "tunnels" to transmit sensitive data through.

A selection of Red Lion's leading automation, networking and cellular M2M products

Overall Implementation Benefits

The efficiency of the Connected Factory, Industry 4.0 and/or IIoT model isn't derived from the sheer volume of connections, but from more valuable connections, and the competitive edge gained by the sharing of information between devices and humans. Seamless communication with operators, control systems and software applications, combined with practical networking options and support for native features and protocols, deliver exponential meaning to data extracted from industrial devices. These capabilities can take automation and remote management to new levels, thereby making this vision a reality.

With the thoughtful integration of supporting components that are designed specifically for this goal, the ability to connect, monitor and control will:

- **Extend equipment lifespan:** increase the value of legacy equipment with powerful protocol conversion
- **Improve process visibility:** gain insight and drive productivity with data logging and communication capabilities
- **Push control to the edge:** scale systems management with control capabilities at the device instead of the central office

These results not only reduce total cost of ownership and speed deployment, but also provide more robust end-to-end functionality across a wide variety of applications.

"The ability to connect, monitor and control extends equipment lifespan, improves process visibility and pushes control to the edge."

The Red Lion Advantage

As the global experts in communication, monitoring and control for industrial automation and networking, Red Lion has been delivering innovative solutions for over forty years. Our automation, Ethernet and cellular M2M technology enables companies worldwide to gain real-time data visibility that drives productivity. Product brands include Red Lion, N-Tron® and Sixnet®. With headquarters in York, Pennsylvania, the company has offices across the Americas, Asia-Pacific and Europe. Red Lion is part of Spectris plc, the productivity-enhancing instrumentation and controls company. For more information, please visit www.redlion.net.

red lion®

Americas
sales@redlion.net

Asia-Pacific
asia@redlion.net

Europe, Africa
Middle East
europe@redlion.net

+1 (717) 767-6511

Connect. Monitor. Control.

www.redlion.net

ADLD00444 120215