WHITE PAPER

The Plant Manager's Guide to IIoT Connectivity

Thomas Nuth
Global Manager, Smart Factories

MOXA®

Abstract

The Industrial Internet, whether it is referred to as "Industry 4.0" or the "Industrial IoT," is for many seen as a broad topic that offers more conceptual ideas than realizable solutions. However, for those involved in factory automation, where factories are becoming smarter, more connected, and autonomous, it is already becoming a reality with big benefits for production quality, asset optimization, safety, and cost reduction. Moxa is one of the few product manufacturers and solution providers that are helping to turn IIoT concepts into a reality on the factory floor.

The purpose of this white paper is to clearly define what Industry 4.0 and the Industrial IoT are and then offer a practical guide for operators and plant managers in implementing realizable Industrial IoT solutions for their own plant or factory. In addition, the operational tools and assets that are available to plant operators to facilitate network connectivity will also be considered.

Introduction

Defining the Industrial Internet of Things: Whether you refer to it as "the Industrial Internet," "the Industrial Internet of Things," or "Industry 4.0," the basic tenets are the same. The industrial Internet describes a progression and unification of technology that offers business-to-business, device-to-device, and people-to-device connectivity across the Internet. Today, automation and IT are combining their advancements of the last twenty years to tackle some of the world's biggest problems in energy, mass transportation, city infrastructure, and manufacturing. In fact, the factory floor is generally recognized as one of the first places for industrial internet exploration and solution realization. Bringing the concepts of edge connectivity, protocol conversion, and edge computing to a position where they can be adopted en masse on the factory floor is certainly easier said than done. Currently, there are three design phases and four IoT enablement steps that are helping plant operation managers tackle the challenges of connecting devices and making factories smarter.

1. **Connectivity:** The Industrial IoT is dependent upon pervasive and fluid connectivity between devices, sensors, and operations control software. In the case of factory automation, the software is known as Manufacturing Execution Software or MES.

   In the past, the division between fieldbus, plant-level networks, control networks, and the application layers of comprehensive industrial operations were clearly defined and separated. This was beneficial for clearly defined job descriptions between plant managers

Released on September 26, 2016

Moxa is a leading manufacturer of industrial networking, computing, and automation solutions. With over 25 years of industry experience, Moxa has connected more than 40 million devices worldwide and has a distribution and service network that reaches customers in more than 70 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for automation systems. Information about Moxa's solutions is available at www.moxa.com.

How to contact Moxa
Tel: 1-714-528-6777
Fax: 1-714-528-6778

Reliable Networks Sincere Service

and IT architects, but it wasn't ideal for operational optimization and scalability. Protocol division resulted in difficulties if a line of CNC machines needed to be connected to the corporations' global control network as it would be complex, expensive, and limited in functionality. Even though this is now gradually changing, it is still very important to understand end devices, protocols, and physical interfaces in order to achieve seamless control from the plant floor to all virtual work stations. In short, connectivity is the first and most critical tenet of the Industrial IoT.

2. **Data-to-Information Conversion:** Today's industrial manufacturing facilities produce lots of data. For example, in automobile manufacturing facilities, up to 8,000 devices can be connected to a single network. In consumer product manufacturing, this number can exceed 12,000. In both circumstances, motion and position sensors are increasingly becoming connected themselves, traversing the PLC barrier. After these nodes are connected, the challenge is putting all that data to work. For many years, enterprise data companies utilizing data clusters have tried to bring the power of Big Data from the digital B2C space to industrial automation but so far with limited success. This has been largely due to a lack of connectivity, the complexity of manufacturing facilities, and the massive amount of data produced in a typical manufacturing enterprise. That said, recent improvements in increased industrial network bandwidth and the utilization of modulated edge computers have allowed factories to scale easily to meet the influx of data. This is why due diligence must be paid to estimating bandwidth demand and selecting a networking vendor that can meet this demand. In addition, your manufacturing operation data requirements must also be met as they continue to grow over the coming years. Existing operators can quickly deploy smart solutions that allow for localized real-time analytics that bridge the communications gap between the LAN on the factory floor, the control LAN, and enterprise networks. Factory operators are beginning to realize that ensuring increased connectivity between the field/plant level and the enterprise can have significant benefits. For example, according to a recent study on Industry 4.0 by McKinsey & Company, a global mining operator was able to translate localized data collection into optimization measures for its chemical processes that increased yield by 3.7%, equating to about $20m annually.

   Due to the huge amount of data that a network of meters can produce in one day, the transfer and storage of that data is often seen as too difficult to facilitate across an industrial network. However, with the advancement and increased affordability of embedded computers and industrial wireless networks, the processing and storage of "stream data" is allowing small- to large-scale manufacturing operations to log years of production data with ease, quickly alerting the central control room in real time if any anomalies occur. The benefits of this *Data-to-Information* capability at the edge of industrial networks has allowed companies to extend product lifetimes by years, while shedding light on potential system failures before they occur. Small investments in industrial connectivity infrastructures have forced the flat-line depreciation model of many process automation companies' accounting teams to rethink their practice, allowing them to lower the bottom line each year and increase value for shareholders as a result.

3. **Cybersecurity Shift:** The cyber level of the Industrial IoT movement is what fundamentally differentiates the Industrial IoT from the IoT. In the industrial Internet, the cyber level serves as a central information hub where data from all field assets and sensors

is stored. It is at the cyber level where customized analytics are performed and largely reside for the purpose of allowing machines to engage in self-learning processes over time. In simple terms, network data is being distributed among the various devices within a local area network (LAN), placing much of the bandwidth and file transfer burden of computation and security evenly among the devices within the LAN. Bandwidth bottlenecks are reduced, as are potential areas of network vulnerability. This is because the cyber level of the Industrial IoT architecture, by its very nature, flips traditional cybersecurity and management models on their head by shifting traffic away from large corporate networks to a network of edge devices and workgroup subnetworks. In this model, each device has a role to play in the security of the greater network and the plant manager has the obligation to construct the network with consideration to redundancy, the strategic placement of firewalls, and the implementation of contingency plans in the event of network failures or network intrusions. The following IoT enablement steps will arm every plant or operations' manager with the correct process for due diligence and consideration when designing a smart factory solution, resulting in a network that is both connected *and* secure.

IoT Enablement Steps:

Goal Identification: Specifying your operational goal is the first step to working towards a solution. However, clearly outlining an operational goal isn't always easy. There is a tendency to follow pre-existing guidelines or follow already established paths when specifying an operational goal. However, this may exclude better, more scalable connectivity solutions before they are even considered. We recommend that the delivery of your operational goal to a supplier or system integrator be as simple as possible so that technical conversations on connectivity and network architecture start at the ground level.

In typical "block and tackle" fashion, make an effort to state your goal in simple, operational terms by first identifying pain points. Then, elaborate step-by-step on what would be required to overcome the operational pain point during each part of your manufacturing process. The first two of the four IIoT connectivity enablement processes, which fall within the identification portion of upgrading or designing a smart factory, are considered below.

Step 1: Assess Your Operational Pain Points

Identify your operational challenges and shortcomings. These could be instigated by environmental or technical causes, or they could be process improvement demands specified by executive management. In short, operational pain points can be specific or broad. They could be as specific as converting one legacy portion of your operation to Ethernet or they could be as broad as lowering company-wide manufacturing costs by 10% within the next five years. For each case, presenting the pain points and challenges up front makes a huge difference for your connectivity provider.

For example:

An operations manager for a machine building company deployed a plant-wide Computer Integrated Manufacturing (CIM) system many years ago. Now, the company has been acquired and its current processes must be integrated into the new company's operations, which includes the MES as well as the operational process control standards. The CIM system installed is not meeting the current requirements and as a result performance is suffering.

Replacing the entire CIM operation is not an option, but the facility must be made more efficient and interoperable with the company-wide operational processes. The operations manager needs a brownfield solution that offers smart I/O condition monitoring that can help optimize their existing CIM and connect to the new MES.

Step 2: Develop and Prioritize Operational Goals

Develop operational goals around your pain points, and prioritize them in order of importance. The objective here is to identify mission-critical solution improvements from those that would be considered benefits. Additionally, prioritizing operational goals will allow you, the integrator, and the supplier to select the most scalable smart factory solution possible. This will ensure that operational goals will be met at the point of project completion, and long-term operational and maintenance costs will be considered as well if there is a need to scale up or down in the future.

Company: IIoT Company

IIoT Goal Planning Worksheet

Step 1: Assess Your Operational Pain Points		Step 2: Develop and Prioritize Operational Goals	
Pain Points	**Goal #**	**Operational Goals**	**Priority**
High equipment failure rate/Increased downtime.	1	Implement preventative maintenance capabilities to help identify potential equipment failures before they occur.	1
Poor alarm management	2	Centralize and customize alarm systems for better management capabilities.	2
Control limitations with equipment	3	Enable high network availability and the ability to monitor and control devices from the cloud.	3
The data from my equipment lacks actionable insights	4	Enable real time analytics and reporting from my existing equipment to enable actionable data insights.	4

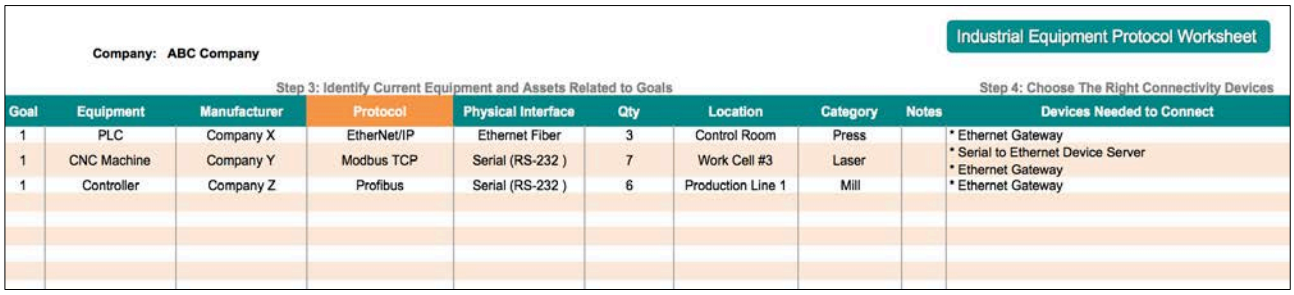
For example:

A plant operator for a beverage company must cut labor costs this year, while seamlessly connecting all legacy bottling lines to the new MES system to allow for more top-level control and visibility at both the control and corporate levels. After determining the main problem was a lack of visibility and control on the plant lines, the plant operator came to the conclusion that the priority was to achieve maximum visibility of all the sensors on lines 1-8 in real time on the plant's MES dashboard. From here, sensors and protocols could be audited to see what solutions and technologies were available to connect various sensors and actuators to the SCADA system, and sensors plus SCADA to MES. Thus, a network audit is required, and should be conducted in conjunction with a distributor, system integrator, or system provider.

Step 3: Understand the Interoperability Status of Key Processes

A central consideration and challenge in achieving a connected smart factory is protocol division. Depending on the specific operation, you may encounter numerous disparate and proprietary fieldbus automation protocols that must be connected to achieve your operational goals. In order to uncover all relevant devices and protocols, work with internal resources and integration teams to record and organize all devices, end nodes, and equipment that exist within your solution space. From this point, register their corresponding protocols, physical interface, plant location, and operational purposes. Also, include any specific limitations or details relevant to the technology, device, or piece of equipment that could be important for a networking supplier or system integrator to know.

Network Audit: Once operational pain points and goals are clearly defined and communicated to all relevant parties, a connectivity plan can be developed. Over the past 30 years, Moxa has taken companies' operational goals from concept to implementation utilizing our expertise as a provider of connectivity and networking IoT solutions. We produce unique solutions, specifically designed for each customer, that adhere to all of the points covered below.



Company: ABC Company

Industrial Equipment Protocol Worksheet

	Step 3: Identify Current Equipment and Assets Related to Goals							Step 4: Choose The Right Connectivity Devices
Goal	Equipment	Manufacturer	Protocol	Physical Interface	Qty	Location	Category	Notes	Devices Needed to Connect
1	PLC	Company X	EtherNet/IP	Ethernet Fiber	3	Control Room	Press		* Ethernet Gateway
1	CNC Machine	Company Y	Modbus TCP	Serial (RS-232)	7	Work Cell #3	Laser		* Serial to Ethernet Device Server * Ethernet Gateway
1	Controller	Company Z	Profibus	Serial (RS-232)	6	Production Line 1	Mill		* Ethernet Gateway

To download this audit sheet tool, please reference the link at the end of Step 3 or at the end of this whitepaper.

For example:

An operations manager is in charge of integrating all motion and positioning sensors and systems that exist in a large automotive production facility into the plant's existing SCADA system, as well as implementing an edge computing solution that will let his operation run analytics in real time on the status of various pieces of equipment. Many of the manufacturing stages within this process are currently controlled in separate networks that all need to be connected to ensure smooth operations. While the current MES can support plant-wide connectivity, there are currently no solutions available that allow for system diagnostics and production analytics on this scale. The operations manager needs to make sure that he can not only support and integrate legacy I/O equipment, but also find the best way to implement edge intelligence in key areas throughout the production process. Also, a substantial increase in bandwidth availability and network redundancy will also be required to support the increased amount of data transferred from sensors to the MES. Finally, redundancy and an industrial routing firewall will need to be designed into the new solution to maintain process subdivision and security. To achieve this, the operations manager must capture all capital assets, sensors, and devices, as well as their corresponding protocols, and catalog them according to their place in the workflow process. From NC Machining to Part Quality Inspection, the operations manager identifies all nodes that need to be included in the new connected solution, along with their associated protocols and physical interfaces.

Moxa offers multiple unique tools to help the operations' manager excel in navigating plant modernization and installing IoT solutions in brownfield and greenfield sites. Download our network audit worksheet to learn more:
http://pages.moxa.com/Industrial-IoT-Connectivity-Workbook.html

Step 4: Choose the Right Devices to Help You Get Connected

Quantify Operational Benefits: The validation process of any investment can be a difficult one, especially to the upper management of a large company when your expertise domain is focused on a particular manufacturing operation that is merely a small part of a much larger business. Uncovering potential hidden costs and savings of a connected, smart factory solution investment requires identification of explicit, as well as projected operational costs and savings.

In addition, by carefully formulating savings projections, combined with a payback timeline on the initial investment, a very strong operational prospectus can be calculated.

For example:

A plant manager in a midsize semiconductor operation has gone through the long and careful process of identifying all of the devices in the current process flow by inputting the device name, location, protocol, physical interface, and plant location into the Moxa Network Audit Worksheet. Also, the manager has gone one step further and provided drawings and plans that have been developed internally. Since the manufacturing facility's pains and operation goals have already been specified, the plant manager is able to select from a number of connectivity solutions providing a gradient of bandwidth, edge computing capabilities, and redundancy levels. Now, the plant manager is able to examine the best solution for his business needs armed with the knowledge that a number of solutions exist that offer different benefits. The plant manager must consider the highest ROI possible with considerations to reduce downtime, labor costs, and the total cost of ownership, as well as maximizing output.

Based on three decades of experience supplying connectivity and networking solutions to the automation sector, Moxa has a unique understanding of the numerous factors that make an investment in a smart factory realizable and practical. While an internal corporate process is likely to be engaged, and is recommended, Moxa offers a toolkit that can be customized and applied to a broad set of scenarios and factory automation sectors. We think this will help you make sure that no technical or cost considerations go unconsidered when you validate an investment decision to internal stakeholders. The payback calculator can help you:

- **Calculate the cost of downtime**
- **Estimate the annual savings with your IIoT investment**
- **Calculate the payback period on your IIoT investment**

Smart Factory Payback Calculator Tool:
http://pages.moxa.com/IIoT-Payback-Calculator.html

Industrial IoT with Moxa:

Ultimately, a smart factory must be a profitable factory: In order to make the Industrial IoT movement a reality on a massive scale, many disparate technologies and industries must learn to work more cohesively with one another. Moxa is a leading industrial networking connectivity company that has grown based on its success providing connectivity solutions for multiple vertical markets. Moxa has connected over 40 million devices, and has witnessed the power that bringing data-driven decision making to the field or factory floor can provide to lowering the bottom line and raising profits by securely connecting previously isolated industrial serial networks to the industrial Internet. Learn more about Moxa by downloading our IoT Connectivity Workbook and Network Audit Sheet at:

http://pages.moxa.com/Industrial-IoT-Connectivity-Workbook.html