How to Get Your Industrial Internet of Things Prescription
Easy Access to the Industrial Internet!
From the field-level directly to the cloud

netIOT
Industrial Cloud Communication

- Don’t “rip-and-replace”—Maintain existing networks
- Move data from devices to cloud applications
- Integrate IoT protocols in all field devices
- OPC UA and MQTT compliant communication
- Multi-protocol to multi-cloud solutions

To learn more about network solutions from Hilscher, call 1.630.505.5301, email: info@hilscher.us or visit www.na.hilscher.com.
CONTENTS

05 How to Get Your Industrial Internet of Things Prescription
08 Firewalls: The Crucial Component for Network Protection
15 Using ERP to Deliver Real-Time Actionable Intelligence
19 Intelligent Alarming Leverages IIoT to Reduce Risks and Costs
25 Fog Computing: Intelligence at the Edge
34 Debunking Common Internet of Things Myths
39 Asset Management to the Last Device
46 Of Co-opetition and Disruption
53 IO-Link and the Industrial Internet of Things
61 Understanding the Role of Gateways
We drive automation for your success. We are your partner to inspire you. We shape the future together.

→ WE ARE THE ENGINEERS OF PRODUCTIVITY.

Our expertise in automation, both electric and pneumatic, can solve all your motion challenges.

For more information: Call: 1-800-Go-Festo 1-800-463-3786
www.festo.us
How to Get Your Industrial Internet of Things Prescription

BY ERIK DELLINGER
Product manager, Kepware Technologies

To correct the disconnect between the market perception of the Internet of Things and what it really is, it’s helpful to think about it in the way a doctor prescribes medications or therapies—it all depends on the specific nature of the ailment.

In recent years, the number of manufacturers leveraging the Industrial Internet of Things (IIoT) to improve productivity, reduce defects and gain more visibility into the operation of their facilities has increased dramatically. A recent survey conducted by PricewaterhouseCoopers (PwC) found that over one-third of U.S. manufacturers consider it “extremely critical” to have an IIoT strategy implemented in their operation. Similarly, a survey from LNS Research found that 34 percent of companies are currently adopting IoT—a figure that will undoubtedly continue to grow in the coming years.
As part of my daily work, I speak with many organizations looking to adopt IIoT. One observation I’ve made with a handful of these companies is that they fundamentally misunderstand how the concept should be applied. Instead of simply treating IIoT as a means of interconnecting devices, lowering operational costs, increasing throughput and enhancing visibility, they perceive it as a silver bullet that will help solve problems they didn’t know they had. This has led to an increased demand from customers to identify new and detailed use cases that demonstrate how IIoT can be applied to a facility or process, which can be like trying to find a needle in a haystack in these early days of IIoT adoption.

The situation can be likened to a visit to the doctor. Patients don’t expect the doctor to guess what problem or illness they have. Neither do they walk in and ask for the best new medicine on the market to cure all of their problems. They give a detailed description of the problems they are experiencing and the doctor prescribes a specific treatment and/or prescription to address it.

It’s this process that companies should think about when looking to implement a solution, whether they call it IIoT or not. In some cases, adopting a more advanced automation system does have the potential to create a new use case, business model or competitive
advantage. For example, one of our customers recently added remote monitoring to their equipment so they can better service it for their customers. Now they offer more than just equipment—they offer a means to improve uptime.

The high-level problems that IIoT helps solve are relatively consistent across all industries (e.g., increase asset utilization, improve productivity, optimize the supply chain, improve product quality, enhance security, etc.). Users look to solve those problems with one goal in mind: increasing profitability. The difference from one use case to the next will lie in the particular IIoT solution implemented—not unlike how a doctor prescribes the latest and greatest medications and/or therapies to patients depending on the specific nature of their ailment or disease.

In some cases, adopting an IIoT solution will offer additional functionality and flexibility compared with a traditional industrial automation system; however, the benefits it provides will be unique to the individual operation, facility or process where it is being applied. I believe the major disconnect between use cases and IIoT for some manufacturers lies in the simple fact that IIoT is not a technology. With that in mind, let’s start thinking about solving problems by applying the latest and greatest technologies—then we can call it IIoT.
Firewalls: The Crucial Component for Network Protection

BY JEFF LUND, TOBIAS HEER AND OLIVER KLEINEBERG
Belden’s Industrial IT Division

Understanding firewalls and the role they play in Industrial Internet of Things applications is key to ensuring network security and resiliency.

With the implementation of the Industrial Internet of Things (IIoT) comes more devices, more data and more interconnections between the plant floor, the IT department and the Internet. All of these factors make industrial cybersecurity, which is already important, even more so. The interconnection between networks and external devices brings about new threats from all angles and in many forms—not only in the form of a larger threat surface for external attack, but also an increased opportunity for device failures, software bugs or user error, all of which can negatively impact the operation of a system.
Firewalls: The Crucial Component for Network Protection

Firewalls are essential for ensuring network security and increasing system robustness and resiliency. No security model is complete without them. Just like the diverse range of devices found across an IIoT network, firewalls come in many different forms, not only in terms of hardware features and industry approvals but also with different filtering capabilities.

Though a firewall might sound like a single type of device, there is actually a diverse collection of device types—which leaves you with the task of determining which type of firewall is best suited for each portion of your application or environment.

**What are firewalls?**

Firewalls protect networks and devices, such as industrial PCs, control systems and cameras, from unauthorized access by preventing network traffic to or from these systems. They are a core element of segmenting a network, and they play a crucial role in any IIoT-related network security strategy.

Firewalls have a few main goals, including:

- Protecting any connections between enterprise and industrial networks, and preventing external threats.
Firewalls: The Crucial Component for Network Protection

• Creating barriers within a network to prevent internal issues from spreading.
• Permitting only approved communications between devices to protect against malicious attacks and device or operator errors.

Firewall devices, like the ones shown here from Belden, are essential for ensuring network security and increasing system robustness and resiliency.
To achieve these goals, firewalls take many different forms, from simple packet filtering to specialized industrial protocol support. For proper network protection and performance, you need to select the appropriate type of firewall for use in each part of your system.

Four considerations when selecting firewalls

There are a variety of factors to keep in mind when looking at options for firewall security. Filtering differences, network environment concerns and how to manage firewalls across a network should be standard considerations for anyone in search of a firewall solution.

Following are four specific aspects of firewall use to keep in mind:

1. Tailored for your network: Like choosing specific IIoT devices, firewalls should be able to accomplish very specific tasks that support your custom needs and applications. Select firewalls that match the unique communications patterns and needs of the devices across the network.

2. Inspection at multiple levels: Depending on where it will sit in your system, various filtering mechanisms will be needed. Firewalls used close to machines as part of a zones and conduits security strategy will need to understand industrial protocols and perform deep packet inspection. In contrast, a firewall used to secure the perimeter between a remote site and the Internet will need the ability to process Internet Protocol (IP) traffic.
Firewalls: The Crucial Component for Network Protection

3. Withstand robust environments: Depending on your network environment, firewalls could be subjected to extended temperature ranges, significant vibration and other environmental factors. Ensure any firewall you choose can withstand harsh environments and that they are compliant with all industry standards and approvals. Selecting a firewall without the robustness required for the application will derail a project very quickly.

4. Keep it simple: Without a powerful management tool for simple and mass configuration of firewalls, the tasks can be very time-consuming and error-prone. Teams need to be able to effectively manage and configure the devices when using multiple firewalls. It’s important that firewalls can be centrally monitored by network management tools to keep things running smoothly.

Firewalls are just one component of an effective security strategy for companies taking advantage of the IIoT. But don’t downplay their use—they are the cornerstone that holds a holistic security model together. Having a solid understanding of the types of firewalls available and the role each plays results in successfully securing the network from a range of internal and external threats lurking out there.
Firewalls: The Crucial Component for Network Protection

By implementing a holistic defense strategy that includes firewalls, you can design networks that effectively mitigate threats and defend against the errors and vulnerabilities introduced by an ever-expanding range of IIoT devices and environments.

To learn more about the various types of firewalls available, read the white paper “Understanding Firewall Technology for Industrial Cybersecurity” (http://awgo.to/682).
It’s About (up)Time.

Upgrade to More Uptime.

When you choose a PROFINET network, the comprehensive diagnostics are ‘baked in’ the protocol. PROFINET diagnostics uniquely help prevent and reduce unplanned downtime. Scalable network redundancy is as easy as running the cable. Because it’s about time.

Welcome to The PROFINET of Things...We’ve Been Waiting for You.
PROFINETuptime.com
Manufacturers are facing a barrage of information about how new disruptive technologies will change the face of their industry. But for manufacturers to embrace these technologies—such as mobile, social, analytics, cloud and the Internet of Things (IoT)—they must have a clear understanding of the technology value-add within the context of today’s business environment. This is what I like to call “purposeful innovation.”

Big Data and the IoT as technology concepts are exciting, but what do they mean to manufacturers from a practical application perspective? As digitization becomes common on the manufacturing floor, there

To realize the full value of Big Data and Internet of Things initiatives, manufacturers need the ability to contextualize data and integrate it into downstream process flows—which is exactly what ERP does.

Using ERP to Deliver Real-Time Actionable Intelligence

BY HIMANSHU PALSULE
Chief technology officer and executive vice president, Epicor Software
Using ERP to Deliver Real-Time Actionable Intelligence

is great potential to improve responsiveness and agility, and adapt more quickly to customers’ changing needs. As more digitally controlled technologies are introduced, we build more connections. As we become more connected, we generate Big Data. And as the volume of data grows, we need new and faster ways to drive insight and actions, and easier ways to arrive at decisions.

So while these disruptive technologies are expected to improve responsiveness, they create new challenges in managing an increasingly overwhelming volume of data that must be converted into actionable intelligence. Manufacturers cannot afford to allow these technologies to inadvertently slow them down.

When it comes to the IoT, it’s not so much about the data as it is about what you can do with that data. As industry analyst Nigel Fenwick at Forrester Research has said, “It’s important to note that digital isn’t just about gathering new external connections; it’s about having the operational agility to act on them.”

Some manufacturing purists might argue that IoT isn’t new to them. After all, machines have long used sensors to report information back to the user—just like the ubiquitous laser jet printer that tells you exactly how much ink is left and where to order replacement
Using ERP to Deliver Real-Time Actionable Intelligence

cartridges. What’s new is that we now have the technology to enable the integration of information across the entire product lifecycle—from design, through engineering, manufacturing, delivery and service—to deliver immediate and actionable information to the necessary departments and functions with greater speed, accuracy and efficiency than ever before. Imagine the new printer that prints your production schedule at the beginning of the shift when it detects you have arrived on the shop floor and automatically emails you a PDF of that schedule.

This is about gaining instant access to information in context to the task or decision at hand. The value-add is aggregating data quickly to make meaningful decisions today that manufacturers couldn’t make yesterday. What’s new and notable with the IoT is this ability to aggregate data, analyze it and use it for predictive modeling.

With all this talk about the IoT, manufacturers may wonder: Where does enterprise resource planning (ERP) fit into this new digital frontier? The reality is that ERP is more relevant in this equation than ever before, as it’s the key to unlocking the value of IoT. To be able to realize the full value-add of Big Data/IoT initiatives, manufacturers need the ability to contextualize data and integrate it into downstream process flows. This is what ERP has always done; however, today’s
CONTINUED

Using ERP to Deliver Real-Time Actionable Intelligence

next-generation ERP platforms are more approachable and more powerful than ever—functioning as the fabric that connects people, processes, data and things in an intelligent and strategic manner that allows manufacturers to create value from new data streams.

To do this, ERP systems must be reimagined to meet the needs of new and emerging technologies in the business of manufacturing. Responsiveness demands simplicity and mobility, with tools designed to meet the specific needs of specific users. It demands new levels of collaboration throughout the supply chain, inside and outside the enterprise. It demands choice in the way information is presented, applications are accessed, and solutions are deployed. With an ERP system that delivers this, manufacturers can check off a big box on their IoT readiness checklist and make good on the promise of real-time actionable intelligence.
What’s the biggest challenge on the plant floor? According to a recent GE survey, managing alarms is still the biggest challenge.

But today, every organization can manage alarms. With intelligent alarming and the Industrial Internet, companies can send the alarms that matter, when they matter, to the right person. Engineers and operators can receive prioritized alerts with instructions, helping them react to and resolve alarms quickly.
By adding geo-awareness to alarming, companies can make intelligent notifications possible and deploy alarms in a geo-context. The right information finds the right person in the right location, which is drastically different from the traditional SCADA world and drives faster action.

In addition to deploying alarms based on location, today’s HMI/SCADA also can filter alarms to increase efficiency. According to analysts, 75 percent of all alarms are noise, and many companies want to examine their systems and reduce the number of alarms. Even with these good intentions, integrators and in-house engineers often need to add new alarms—creating a seemingly unending cycle of alarm creation and reduction.
As a result, companies are forced to accept that there will always be a certain level of noise from alarms, and operators must know what to pay attention to and what not to pay attention to. A problem arises with temporary staff operating machines or new operators coming on board. The temporary or new personnel don’t have the experience to filter through the alarm noise and make sense of it.

With intelligent alarming fueled by the Industrial Internet, companies can take all of the raw alarms in underlying systems and apply a level of analytics to them. Modern HMI/SCADA systems can deliver the right alarm, perhaps even a derived or intelligent alarm, to mobile devices rather than simply transferring confusing raw data.

Furthermore, fourth-generation HMI/SCADA can add a layer of proactive analysis to deliver predictive intelligent alarming. Today’s technology isn’t just about delivering the right information after an event has happened; it is also about delivering information before a catastrophic issue occurs and preventing it from taking place.

Consider temperature monitoring on a piece of equipment. If the temperature exceeds the upper control limit, an alarm is activated. Traditionally, an operator would now react to the alarm. Analytics have made it possible to evolve from being reactionary to predicting
when the event will occur and taking steps in advance.

As an example, a food manufacturer can monitor the temperature data point, put an analytic on it and predict the temperature based on a statistical model. The company can push an alarm to an operator to ensure that action is taken faster before a batch is ruined.
Intelligent Alarming Leverages Industrial Internet of Things to Reduce Risks and Costs

This applies to other industries as well, such as pharmaceutical with multimillion-dollar batches of product, as well as maintenance events on discrete equipment. The application of predictive knowledge, delivered as an intelligent alarm in a geo-aware context, is far-reaching and offers new possibilities for consistently optimized operations.

Enabling smart operators

Today’s HMI/SCADA is not just monitoring and visualization with alarms rolling in. For operators, HMI/SCADA is their decision support system and alarm management is critical.

Here are two golden rules to think about:
• Don’t allow technology to complicate the operator experience.
• Use technology to improve the operator experience and manage alarms for greater efficiency.

With just a glance, operators should be able to recognize which information requires their attention and what it indicates. You can enable smart operators with intelligent alarming for faster alarm detection, greater understanding and improved business outcomes.
It’s often difficult for industrial operators to collect data from their devices in a format that is compatible with advanced software platforms. Moxa’s 4G LTE Jump Start Kit provides an easy, scalable, and cost-effective solution to bring industrial sensors and devices into a management platform or database.

4G LTE Jump Start Kit
- Programmable 4G LTE data logger
- Modbus gateway
- I/O module supporting analog and digital inputs
- Verizon 4G LTE module and accessories

Learn more at pages.moxa.com/4GKIT
On the train to work, Lee opens an email on her smartphone sent from a programmable automation controller (PAC) operating a surface-mount tool at her factory. The PAC has attached a quality control report to the email that suggests changing the tool’s solder temperature.

To generate that email suggestion, the PAC had securely sent yesterday’s production data to a cloud-based analytics system to compare current and historical data for the machine. Next, it accessed the machine manufacturer’s website and obtained the latest recommended settings. Finally, the PAC built a production efficiency report with a suggested solder temperature for today’s production run that would increase yield by 7 percent over yesterday’s run.

To achieve the business benefits promised by the Internet of Things, three core problems must first be addressed.
Lee clicks a link in the email and connects to the PAC’s mobile interface over a secure, encrypted channel. She logs in and navigates to the machine’s solder temperature set point, where she enters the recommended value.

**All this takes place before she gets to the office.** That PAC operating the surface-mount tool at Lee’s factory operates at the edge of the factory’s network. Systems like these at the network edge are increasingly able to leverage cloud-based resources to perform fog computing—where computing resources exist as needed along the path from a sensor to the cloud to reduce the total amount of data that needs to be sent to the cloud for storage, processing and analysis. As a result, businesses can more quickly identify real opportunities for operational efficiency improvement and meaningful revenue generation.

To foster such business benefits, data from the physical world of machines and equipment must be available to the digital world of the Internet and information technology (IT) systems, quickly, easily and continuously. Successful IoT applications require operational technology (OT) professionals to make data from their systems—which monitor and control the physical world—accessible to the data processing systems of IT professionals.
Once the data is there, cognitive prognostics algorithms running on IT systems can analyze it, refining raw physical data into actionable information that can predict outcomes in real time. The results can be used to improve inventory management and predictive maintenance and reduce asset downtime.

But before such benefits can be realized, three problems need to be solved.

**The Big Data problem**

As we connect more devices and systems in our plants to the Internet and build out the IoT, a tremendous amount of data will be generated and transmitted—terabytes of data per second. These are volumes of data the digital world has never seen before. This is the Big Data problem.

Moving that much data onto existing network and Internet infrastructures for cloud-based analytics and centralized management will dramatically increase Internet latency. For many industrial IoT applications, latency is not acceptable because real-time control and monitoring are mandatory.

For IoT to reach critical mass, intelligence must be pushed to the edge of the network. The network edge is where physical assets
(things) such as sensors, actuators and circuits are connected to the network. Fog computing brings computation capabilities closer to the network edge to filter or process data and send only required data to the cloud, thereby decreasing traffic and latency on local networks and the Internet.

Fog computing also plays a valuable role in efficiency, security and compliance. Industrial fog computing systems are also responsible for the local process control and automation tasks of traditional industrial applications.

The connectivity problem
At the network edge, OT assets like motors, pumps, relays and meters are attached to industrial equipment and machines. These assets translate what’s happening in the physical world (temperature, light, vibration, sound, motion, flow rate) into electrical signals like voltage and current, which are then interpreted by other systems to monitor and control physical equipment and machines. They were not designed to communicate with the IoT.

Assets like these rarely connect to the Internet, let alone speak or understand the protocols and languages the Internet uses, like Internet Protocol (IP) or RESTful APIs. They don’t have a built-in TCP/IP stack or a web server. And they have little or no built-in computing
power for the fog computing required to filter volumes of data before sending it to the cloud.

As a result, the Internet and the things we want to connect to it aren’t communicating. There’s a disconnect between the physical world of currents and voltages and the digital world of data and communications.

**The IoT architecture problem**

In today’s IoT architecture, for a cloud-based server to capture data from an analog sensor, the sensor’s data must be translated to digital data. In some cases, these sensors are physically wired to controllers such as PLCs.

However, PLC hardware, software and programming languages were designed for repetitive, application-specific tasks like process control and discrete automation. They typically use proprietary protocols and languages for communication and programming, lack information security standards like encryption and authentication, and were originally designed as standalone systems without Internet connectivity in mind. Systems that use Internet-compliant communication protocols such as PCs, web servers and databases require vendor-specific and often proprietary middleware or hardware-based protocol gateways to communicate with a PLC.
OPC software is one solution, but it was designed using the Microsoft Windows-only process exchange called COM and DCOM. Most systems and devices connecting to the IoT, such as sensors, relays, smartphones and web servers, are not Windows-based. For example, Apple and Android smartphones run modified versions of the Linux operating system, where COM/DCOM process exchange does not exist. OPC UA (Unified Architecture) has been released to address this problem, but it typically relies on legacy OPC drivers built on Windows architecture. One option is to embed an OPC UA server into IoT assets, but the fact is that modern web servers, databases, smartphones and tablets don’t natively speak OPC UA.

PLCs, OPC servers, proprietary drivers and protocol gateways quickly become layers of complexity that require time, money and specific domain expertise to install and support. With this approach, data is converted so many times that data integrity and security can be jeopardized, and provisioning and troubleshooting is very difficult.

Multiply these issues across the billions of devices we expect to connect using the IoT and you see the communication challenge the IoT faces.
A better way

For the IoT to reach critical mass, layers of complexity must be removed from the communication process between digital systems and physical assets. Today’s Internet uses a common set of protocols, tools and routines designed to make data transportation, acquisition and analysis a seamless process. We can collect meaningful data from the huge installed base of existing things, but it requires a solution that understands both sides of the OT and IT equation, meaning that it must be able to:

- Translate the physical world of currents and voltages (OT) into the secure RESTful APIs and JavaScript Object Notation (JSON) frames the digital world (IT) understands.
- Process and filter mountains of data, sending only pragmatic data to the cloud.
- Communicate using open Internet protocols such as HTTPS or MQTT over TCP/IP.
- Provide enough processing power to maintain the closed-loop, real-time control requirements of industrial applications, along with edge computing capabilities.
- Deliver all of the above in a package suitable for challenging industrial environments where dust, moisture, vibration, electromechanical frequencies and temperature vary widely.
The IoT will fall short of its potential until communication, security and computing technologies of the Internet find their way into computing at the edge. That’s why fog computing can be the sensor on ramp to the IoT.

Fortunately, Internet technologies are available in some industrial systems today. And some vendors have already started bridging the gap between OT and IT by adding IoT technology like HTTPS and RESTful APIs directly into PACs.

Our shortest path to a successful IoT is to leverage the existing interoperability technologies of the Internet in industrial automation products and applications.
NETWORKED VALVE CONTROL. COMPACT. FLEXIBLE.

WAGO-I/O-SYSTEM 750 750-632 Proportional Valve I/O Module

• Compact, 12 mm wide module
• Control two valves up to 24V and 1.6A each
• Integrate with a variety of networks and I/O modules

www.wago.us/valve_control
Debunking Common Internet of Things Myths

BY COLIN GEIS
Director of product management, IIoT, Red Lion Controls

One of the most common myths is the idea that existing assets are not capable of connecting with cutting-edge platforms and therefore should be replaced.

The Industrial Internet of Things (IIoT) is often focused on the benefits of connecting assets to provide granular visibility into processes with the hopes of driving operational efficiencies across organizations. When sensors and equipment are connected, data can be more effectively collected, analyzed and turned into actionable intelligence. This gathered intelligence provides insights into trends, exceptions and predictions that help organizations make more informed decisions and better allocate resources.

But how does an organization get to this point?
Debunking Common Internet of Things Myths

One of the most common myths associated with IIoT technology is the idea that existing assets are not capable of connecting with cutting-edge platforms and therefore should be replaced. The reality of pursuing a costly “rip and replace” approach to achieve the benefits of the IIoT requires significant resource investment in the form of longer, more complex implementations.

Instead, organizations should consider leveraging existing assets to provide the foundation for effective IIoT deployments. In fact, many IIoT-ready methods exist for the quick connection and collection of data from legacy equipment. These methods include physical media conversion, protocol communication and sensor deployment strategies. Each of the following IIoT-ready approaches not only addresses common obstacles associated with device obsolescence, but also extends equipment lifespan:

- **Physical media conversion:** Though newer and more efficient cabling—such as Ethernet or fiber optics—exists for long-distance IP communication, many traditional industrial environments still predominately have serial cabling connecting equipment. It is important to note that, though serial cabling is typically required for local process communication, it is a poor choice to be natively retransmitted over larger IP networks because of issues such as device polling, network
latencies and potential packet loss. This is one of the main reasons why physical media converters can play an important role in connecting legacy equipment to upstream platforms.

- **Protocol communication**: With so much local equipment communicating via serial cabling—often using Modbus or other proprietary manufacturer protocols—protocol converters provide another way to connect serial environments to more IP-friendly protocols that perform better in larger networks and extend well outside of factories. Protocol communication is becoming even more important with the introduction of IIoT cloud platforms, which typically use very lean Internet protocols for the continuous collection of data from hundreds or thousands of heterogeneous devices.

- **Sensor deployment**: When existing equipment lacks communication capabilities, or equipment data is not easily accessible, sensors can be used to collect operational information. Organizations can either leverage existing sensors or install new ones to collect data from legacy assets. Although this process might cause minor process downtime, organizations are able to eliminate asset obsolescence while also realizing the benefits of granular data collection via strategically placed sensors.
Using these deployment strategies, existing assets can now physically connect and communicate with a range of protocols capable of exchanging data with cutting-edge platforms. This approach provides a solid foundation for IIoT implementation that enables organizations to seamlessly collect and analyze operational data to help make better-informed decisions relating to production efficiency, asset utilization and waste reduction. By integrating IIoT-ready tools and technologies into existing processes, organizations can cost-effectively take advantage of existing assets to drive future IIoT success.

Red Lion Controls is a U.S. manufacturer of industrial automation and networking solutions that help organizations connect, monitor and control assets worldwide. Visit www.redlion.net to learn more.
Extract Your Machine Intelligence with Advantech’s Industrial IoT Gateways

Seamless Connection, Aggregation, and Transmission
Advantech’s wide selection of Industrial IoT Gateway Solutions are designed with Industry 4.0 technologies in mind. With their advanced communication capabilities, these smart factory solutions make connection to the cloud easy.

Compact Edge Computing Gateway
UNO-1200 series
UNO-2200 series

Intelligent RTU
ADAM-3600 series

Industrial Control Computer
APAX-5580 series

Wireless I/O
WISE-4000 series

IoT Dashboard Software
WebAccess

www.advantech.com
Asset Management to the Last Device

BY MICHAEL BOWNE
Director of technology marketing, PI North America

How the concept of asset management is evolving with the Industrial Internet of Things to address assets ranging from robots to I/O blocks.

The cutting-edge thought process in manufacturing today is to use the automation network for more than just automation. That could mean using it for safety, energy management, embedded web servers or asset management. Asset management might be considered “old hat” in the manufacturing space, but under the influence of the Industrial Internet of Things (IIoT), new life is being breathed into the topic.

What's new is the extent to which asset management is evolving. It’s not just about factory lines or cells or even individual machines anymore—it’s now coming down to singular devices.
There are two main drivers behind this development. The first is the installation of Ethernet into the farthest reaches of the network. This allows asset management information to be retrieved transparently. The second is the increased ease with which data can be mined,

Programmable alarm states enable predictive maintenance.
To achieve the benefits of asset management for connected devices as a profit driver, you must leverage the information stored in memory on the device. This means complete information on a device can be gathered, not just fragmented pieces.

The benefits of asset management for connected devices as a profit driver are well known, but to achieve this you must leverage the information stored in memory on the device. This information falls into two categories: identification data (I-data) and maintenance data (M-data). Together, this I&M data contains all the required information needed to label, locate and describe a networked device.

The device can be anything: a robot, a motor, a valve or an I/O block. I-data records contain read-only information about the device like the serial number, hardware version and software version. M-data, on the other hand, is read-write data written at the time of installation, such as a plant-wide unique identifier, location or installation date.

The best way to understand the usefulness of I&M data is through example. Consider a network with multiple instances of the same type of robot. These robots could have been installed at different times or upgraded along the way. Performing an I&M audit quickly informs a maintenance manager that some of the robots do not have the latest firmware version installed. This is particularly useful in large networks, where I-data makes it easy to distinguish similar
DO MORE WITH YOUR DATA

Introduce real-time industrial data to your cloud-based business systems with Kepware’s industry-leading communications platform.

Kepware Technologies provides a portfolio of software solutions that connect diverse industrial automation devices and software applications. Established in 1995 and now distributed in more than 100 countries, Kepware has helped thousands of customers improve operations and decision making.

Visit us online to learn more about our communications platform that’s enabling the Internet of Things.

KEPWARE.COM
Asset Management to the Last Device

devices from each other. In general, it’s best to think of I&M data as a traditional nameplate, but smarter and in electronic form.

M-data is not only written during device installation, it is also acquired during production. Critical components can trigger a flag when certain preset maintenance conditions are met. Typically, this involves an extended traffic-light model to display device states. In addition to the standard failure state, pre-warning levels such as “maintenance required” and “maintenance demanded” are also employed. For example, if a plant manager knows the valve will degrade after 10,000 actuations, a “maintenance required” flag is set after 8,000, and a “maintenance demanded” flag is set after 9,000. This can help eliminate costly unplanned downtime.

Many of these concepts are not new, having been part of the Profinet specification for a decade. In the ISA-95 hierarchy, I&M data is passed from the field level to the manufacturing execution system (MES) level and to the enterprise resource planning (ERP) level. With many IIoT futurists predicting a transformation of that hierarchy into a flatter network architecture, the connection from field-level systems to MES and ERP systems will become more transparent and direct. Therefore, the focus of asset management needs to expand to include the network to which those devices are connected.
Because a factory’s automation network is used for more than just automation, it is an infrastructure and an asset unto itself. Just like I&M data is used to manage the assets connected to a network, there are tools available to manage the network as an asset. Due to the proliferation of Ethernet at the office level, its adoption at the field level allows manufacturers to leverage many of the tools developed for it along the way.

One such tool is the Simple Network Management Protocol (SNMP). It can be used to query Ethernet switches (standalone, or in devices) for many Ethernet-related parameters like bandwidth utilization, retries, link status, etc. Another tool is Link Layer Discovery Protocol (LLDP), which makes it easy to extract the topology of a network. Finally, Hyper Text Transfer Protocol (HTTP)—which is so universal that we almost forget it’s a protocol—delivers the ability to browse web pages in connected devices.
Learn how to prepare your infrastructure for the Industrial Internet of Things.

Join others from across the country at this practical, no-nonsense, hands-on event, and learn how you can start taking advantage of the IIoT.

Registration is now open. Visit www.belden.com/designseminar to learn more about the hands-on labs, live demonstrations, guest speakers and breakout sessions.

If you’re involved in designing or maintaining industrial Ethernet networks, this event is for you. You’ll walk away with the information and skills you need to excel with mission-critical networks – from network design and security to wireless, redundancy and more.

www.belden.com/designseminar
#BeldenDSx16
The Internet of Things (IoT) is thankfully through its hype cycle and reality is upon us. Quietly, a revolution has begun and some hard truths are visible. One of these truths deals with something we in automation know a lot about—the mysteries of communications standards.

In home automation, IoT is seen to be cool, even useful in some cases; but many different systems are being offered and interoperability is an issue that’s slowing everything down.

In industrial automation, we have learned to accept a variety of protocols. My own company knows this better than most because...
IIoT Advantage: Remote Monitoring for Edge Control

Red Lion's rugged RAM® cellular RTUs push control to the network edge with an easy-to-configure event engine that simplifies remote asset monitoring regardless of location.

- Trigger I/O or send SMS text message alerts based on real-time operational data
- Address harsh environmental conditions with rugged, secure all-in-one platform
- Support varied connectivity options from I/O to serial, Ethernet and Wi-Fi

Learn more today at www.redlion.net/RemoteMonitoring
we’ve built a great global business connecting and interconnecting these standards transparently. Home IoT (to date) seems incapable of replicating the industrial experience, suggesting that it will not gain traction for quite a while.

At least that’s what I thought until I read about Amazon extending the reach of its Amazon Web Services (AWS) dramatically with IoT extensions. AWS is a cloud solution that achieved market superiority by being early and competitive. As one commentator put it: “Like a sleeping giant awakening, over the last six months Amazon gradually rolled out parts of its IoT offering... Amazon is laying the groundwork to be a major force in the IoT, especially in the connected home and office.”

If ever there was a single player with the potential to unify a shaky market, Amazon is it. By offering development kits, analysis packages, data ingestion devices, application program interfaces (APIs) and even an IoT device registry, it could be triggering a major market shift.

Of course, Amazon’s motives are not altruistic. But think of smart home devices communicating over Wi-Fi and the Internet to Amazon’s back end with all its buying and delivery power, and
CONTINUED

Of Co-opetition and Disruption

you can see what might be coming. The Dash Button one-touch ordering system is already operational and the Alexa voice platform is showing further commitment to this market. Now I read that the Echo speaker system has taken off. For the first time, I really believe
that my fridge might be capable of having fresh stuff delivered before I realize I need it!

Will this concept spill into the industrial world? It might. If you can order spare parts or new products simply by pressing a button or shouting at your PC—or have systems order it for you and have it delivered tomorrow—think of the advantages.

Meanwhile, automation vendors and suppliers have not been idle. Hilscher’s contribution to the process has been focused on agreements with major IT suppliers around our Edge gateways. We are collaborating with IBM in John Deere’s pilot Industry 4.0 project, which includes a cyber-physical system and IBM’s Watson technology. Separately, we have developed a partnership with SAP involving its HANA Cloud Platform and Asset Intelligence Network. Both have common aims—bringing together people, assets and enterprise—and both are supportive of Industry 4.0 and Industrial Internet Consortium values and methods.

Both projects demonstrate that a collaborative process is growing. Better cooperation between IT and the plant-floor operational technology (OT) will be needed. Also, I suspect, better collaboration between natural competitors—the so-called co-opetition option whereby competitors
learn how to work together for mutual benefit when necessary—will increase. This has been happening in IT for a long time, and I predict it will become more common in our industry too.

Another factor becoming clear is the potentially disruptive nature of Industrial IoT (IIoT). Disruption is a word we hear a lot in consumer markets (such as Uber, Airbnb, PayPal, etc.), but it’s an unwelcome word in automation. Rest assured control won’t change (except hopefully for the better), nor will the networks and equipment supporting it. Plus, our industry has a great deal of experience interfacing with IT, especially around maintenance and production management. So what’s new or really disruptive about this for automation?

The cold fact is that current PLC architectures are mostly incapable of supporting the data exchanges needed for IIoT. IIoT must therefore work in parallel with existing systems, not on top. It might not be long before Edge gateways linking to the cloud will be commonplace in automation networks and a new market will have arrived. A corollary is that, unless you’ve already gone digital—i.e., you have fieldbus or Ethernet networks already deployed—then IIoT might not be available to you. Be warned!

In industrial automation, we have learned to accept a variety of protocols. Home IoT (to date) seems incapable of replicating the industrial experience.

Of Co-opetition and Disruption
Is Your Industrial Ethernet Network Operating at 1Gbps?

Consider CC-Link IE Field as your open network solution.

GIGABIT INDUSTRIAL ETHERNET
Enabling seamless data communication from the plant-level enterprise network to the production floor network

CC-Link Partner Association – Americas
Tel: (847) 478-2423 or (847) 478-2647
email: info@CCLinkAmerica.org | www.CCLinkAmerica.org
IO-Link and the Industrial Internet of Things

BY NUZHA YAKOOB
Senior product manager, electric Automation, Festo

The vendor-independent interoperability aspects of IO-Link make this non-fieldbus method of connecting plant floor devices and systems an appealing way to jump-start Internet of Things initiatives.

One key to making the Industrial Internet of Things (IIoT) and smart factories a reality is two-way communication between low-level sensors and actuators and higher-level controllers, automation systems and manufacturing execution systems (MES).

IO-Link does just that.

IO-Link enabled devices not only transmit machine data to factory management systems, they let a control system download parameter data to the device, which, in turn, can send status information back to the controller. Thus, IO-Link devices facilitate machine
Maximize Manufacturing Growth

Manufacturers are under constant pressure to meet demanding timelines with little margin for error. Epicor solutions help you uncover potential production obstacles—as well as new growth opportunities—so you always know how your business stacks up.

epicor.com | info@epicor.com | 1.800.999.6995
IO-Link devices facilitate machine commissioning and startup, can make adjustments while a machine is running, and provide monitoring and diagnostic capabilities.

IO-Link is the first I/O technology to be adopted as an international standard (IEC 61131-9) and lets devices from various manufacturers communicate with each other. However, it is important to note that IO-Link is not a fieldbus. It enables point-to-point communication between field devices and the automation system. Traditionally, integrating a fieldbus interface all the way down to the lowest field-level device was expensive. IO-Link is a straightforward and economical system that transmits binary, analog, parameterization and diagnostic data via simple, unshielded three-wire cable.

A basic IO-Link system consists of a master; devices like sensors, valves, motor starters and RFID readers; cables up to 20 m long (typically with factory-assembled M12 connectors); and configuration software tools. The IO-Link master can have several channels, one for each connected device, and it can be integrated into a PLC or controller and serve as a gateway to fieldbuses such as DeviceNet, Profinet and EtherNet/IP. As a result, it serves as the connection...
Key advantages of IO-Link include:

- Automatic detection and parameterization of the IO-Link device. During initial setup, a device’s operating parameters are stored in the master. Once connected, the master recognizes the device and enables automatic startup. If a device like a sensor fails, it can be swapped out and parameterization data stored in the master automatically downloads to the replacement device.

- Device monitoring and diagnostics. IO-Link permits equipment components and systems to be monitored and proactively managed. Diagnostic information supplied by IO-Link devices lets the control system track data and trends, facilitating preventive maintenance and improving machine uptime. In the event of a fault, it pinpoints the problem, thereby making troubleshooting easier. No special expertise is necessary on the part of maintenance technicians.

- Changes on the fly. Parameters can be quickly adjusted for installed devices while the machine is running. For example, consider a pressure regulator controlling the force that a pneumatic cylinder applies to a product. If the next product requires a different force, users can reconfigure the regulator’s pressure set points on the
fly and keep production running. That substantially differs from the conventional, time-consuming process of having a machine operator manually reset pushbuttons or adjustment screws. The ability of the controller to quickly and remotely change device
settings is a key attribute of IIoT. It minimizes the transition time from one type of operation to another and gives machines greater flexibility to handle a wider range of products.

- Reduced spare-part costs. By exploiting the configuration capabilities of IO-Link, one device can be configured to have different output functions—such as a sensor that’s NO or NC.

All these advantages, combined together with vendor independence and interoperability, make IO-Link a significant tool for successfully implementing IIoT and Industry 4.0.

Festo offers a range of IO-Link compatible products, including IO-Link masters, pressure and flow sensors, displacement encoders and position transmitters, valve terminals, proportional pressure regulators and stepper motor controllers.

A few examples include:
- An IO-Link master with CECC controller with four IO-Link ports operates with electric and pneumatic actuators. It reduces installation and networking costs for intelligent sensors and valve terminals and provides valuable diagnostic options.
CONTINUED

IO-Link and the Industrial Internet of Things

• Proportional pressure regulators VPPM connected to IO-Link are used for testing, metering and pressing applications in food, automotive, electronics and light-assembly industries.

• Position transmitter SDAT with an IO-Link interface accurately detects piston position for process monitoring in screw driving, riveting, welding, pressing and clamping tasks.

In addition, Festo has application knowledge in both factory and process automation and can offer basic and advanced training for industrial users.
Internet of Things?

Not so fast! There’s a huge gap between the Internet and your industrial things.

Silosed behind proprietary PLCs and protocols lies valuable operational technology (OT) data that can create new business opportunities and generate profitable outcomes. But how do you securely access, analyze, distribute, and visualize this data?

Opto 22 bridges the gap.

Input/Output. Guaranteed-for-life Opto 22 I/O connects to your industrial things, translating physical world signals into digital data—and back.

Logic. SNAP PAC® programmable automation controllers monitor and control things in the OT world, quickly, reliably, and affordably.

Data. groov processes data at the edge, analyzing, sorting, and distributing it with the data structures and protocols IT understands.

Visualization. groov lets you securely visualize and act on your IT and OT data from anywhere using a mobile device or Web browser.

How can we help you bridge the IT/OT gap? Download our IoT Primer now at opt22.com/iot-primer. Or speak to an applications engineer today: 800-321-6786

www.opto22.com
Until recently, it was difficult for separate pieces of industrial automation equipment to communicate with each other. IMS Research estimates that 85 percent of the legacy devices installed still lack this ability due to the lack of compatibility between different manufacturers. The lack of compatible standards and programming languages meant that gathering all the data in one program was an expensive challenge.

Although many devices haven’t yet standardized their programming, technological advances are enabling manufacturers such as
Understanding the Role of Gateways

Advantech to develop hardware and software that can communicate with and collect data from all manner of devices.

Most new devices on the market offer smart connectivity—i.e., the ability to connect to and be controlled from a wide range of Internet-based devices. They can be easily monitored from web-enabled SCADA management software, such as Advantech’s WebAccess via Ethernet or wireless networks, and increasingly don’t require the services of a gateway.

The challenge that remains for most manufacturers involves the monitoring of disparate legacy equipment with the same software. That’s where gateways play an important role.

Advantech’s solution to this problem has been to design and build cloud-enabled HMI edge gateway computers, such as the UNO-1372G, UNO-1252G, UNO-2200 and APAX-5000 with dual LAN ports, COM ports, CANbus and iDoor modules, for connecting to multiple interfaces. For the oil and gas and water/wastewater industries, Advantech’s ADAM-3600 series intelligent remote terminal units (RTUs) can complete tasks on site and deliver data to the cloud.
CONTINUED

Understanding the Role of Gateways

To help address oil and gas industry-specific legacy device connection issues, Advantech’s APAX-5402-E2A0 2-slot PCI express module, APAX-5490 Local Communication Module and APAX-5090 Remote Communication Module use iDoor Modules to act as vertical gateways.

Advantech Industrial IoT Gateways (from left to right): APAX-5580 Industrial Control Computer, ADAM-3600 Intelligent RTU and UNO-1200/UNO-2200 Compact Edge Computing Gateways.
gateways and convert the protocols from legacy equipment to new management software.

Advantech’s iDoor technology is a modular method of adding flexible functionality to a range of devices. For use in gateway applications, iDoor modules can connect directly to CANBus, Profibus, Profinet, EtherCAT, EtherNet/IP, Sercos and Powerlink devices, saving users from additional purchases of separate devices to stand between the UNO or APAX and the legacy equipment.

By standardizing networking methods and allowing devices to use established industrial networking technologies to communicate via Ethernet, all devices old and new can now be connected to the same network.

Gateways are also essential for the proper flow of status and command information for use by manufacturing execution systems (MES) and enterprise resource planning (ERP) systems.

Once all data from devices/machines has been filtered and converted into a standard protocol, the data can be transferred to servers via the Internet. Factory managers can then oversee the operating status of all machines and systems on all production lines of all of
Understanding the Role of Gateways

their facilities and implement remote management and control. Big Data applications also can be used for analysis to extract meaningful patterns to improve operations.

The next mission for gateways is to bridge the gap between machines and humans. Gateways are responsible for collecting data from machines and translating it into a useful operational status. Advantech’s WebAccess/HMI and its visualized HMI Runtime software, combined with the remote display technology of the UNO series computers, allows operators to diagnose and control machines without being present on site.

Advantech does this in two ways: WebAccess/HMI software provides centralized management of all devices and TagLink helps make the ADAM-3600 an intelligent RTU. WebAccess/HMI software enables data transfer between units and the management system by providing more than 450 PLC and controller communication drivers. TagLink, Advantech’s latest gateway technology designed just for RTUs, converts protocols such as DNP3 and IEC-60870-5-104 to Ethernet. The integrated software takes data from the devices connected to the RTU and allows users to access and view specific information about each of them. The ADAM-3600 acquires the device’s data, performs various calculations and can also diagnose faults. TagLink also allows
Understanding the Role of Gateways

engineers to control a device directly from the web server and transfer its data to cloud servers. With support for more than 200 I/O drivers, it can read information from the most common devices. This data can also be sent to WebAccess, where it can be analyzed in comparison to the data sent from other devices to achieve optimum efficiency.

By offering centralized management to Advantech IP-based devices over HTML5, there is no need for a centralized operation center, since the devices can be monitored across the Internet or intranet from any modern browser. WebAccess/NMS can be used to auto-discover any of the Advantech Ethernet devices on the network and create an automatic topological diagram of the network. If third-party devices are installed, their details can be imported separately and placed manually in the map.

Once we have old and new devices connected and talking to each other, the next step in creating a smart factory is to make the information visible to operators and managers so they can make informed decisions using the data delivered via the HMI's. This will lead to more intelligent factories and greater opportunities for manufacturers.
DRIVE SMART OPERATOR DECISIONS

With just a glance, operators can recognize which information requires attention, what it indicates, and the right actions to take. That’s the power of GE’s high performance HMI/SCADA—enabling operators to transform business through increased efficiency and reduced costs.

Make the best decisions faster.
ge.com/smart-operator